VISOKO UČILIŠTE ALGEBRA

ZAVRŠNI RAD

Rješenje za automatsko izdavanje certifikata

Krešimir Kovačević

Zagreb, listopad 2017.

„Pod punom odgovornošću pismeno potvrđujem da je ovo moj autorski rad čiji niti jedan dio nije nastao kopiranjem ili plagiranjem tuđeg sadržaja. Prilikom izrade rada koristio sam tuđe materijale navedene u popisu literature, ali nisam kopirao niti jedan njihov dio, osim citata za koje sam naveo autora i izvor, te ih jasno označio znakovima navodnika. U slučaju da se u bilo kojem trenutku dokaže suprotno, spreman sam snositi sve posljedice uključivo i poništenje javne isprave stečene dijelom i na temelju ovoga rada“.

U Zagrebu, datum.

Ime Prezime

Predgovor

Želio bih se zahvaliti svom mentoru Vedranu Dakiću na suradnji prilikom izrade završnog rada. Želio bih se zahvaliti i svim profesorima Visokog učilišta Algebra koji su, svaki na svoj način, ne samo posvetili svoje vrijeme da me nauče nova znanja nego su dio svoje mudrosti ugradili u mene i učinili me boljim čovjekom.

Drago mi je i sretan sam jer sam tijekom studiranja upoznao nove kolege i drage prijatelje.

Posebno bih se želio zahvaliti svojoj supruzi Srećki i djeci Luki i Lani, što su me podržavali, motivirali i nasmijavali tijekom studiranja. Hvala im na razumijevanju što im nisam mogao pomagati u njihovom školskom učenju, igrati se sa njima i to što su bili uskraćeni za moje prisustvo tijekom studiranja. Nadam se da će moja diploma biti poticaj, Luki i Lani, da oni jednog dana ostvare svoje pune potencijale, da završe fakultet i da ponosno i sretno koračaju kroz život.

Prilikom uvezivanja rada, Umjesto ove stranice ne zaboravite umetnuti original potvrde o prihvaćanju teme završnog rada kojeg ste preuzeli u studentskoj referadi

Sažetak

Organizacije u svom radu godinama razvijaju informacijski sustav, prilagođavaju ga, unaprjeđuju poslovne procese i omogućuju efikasnije i efektivnije upravljanje organizacijom. Proizvođači softvera kao što su Microsoft, Oracle, Apple i drugi proizvode gotova rješenja koja se implementiraju na velikom broju korisnika te ih sistemski integratori implementiraju u organizacijama. Takva gotova rješenja je moguće konfigurirati pomoću opcija, postavki i setom određenih funkcionalnosti (engl. *Out-of-the-box*) koji su već ugrađeni u proizvode, ali ih nije moguće prilagoditi (engl. *Custom*), u većem opsegu, specifičnim potrebama organizacija. Kako bi riješili specifične zahtjeve organizacija nezavisni proizvođači softvera razvijaju specijalizirana rješenja prilagođena organizacijskim potrebama. Takvo jedno rješenje opisano je u ovom završnom radu. Opisani su zahtjevi organizacije te ciljevi koji su se postavili pred razvoj i implementaciju rješenja. Rješenje je osmišljeno i dizajnirano prema specifičnim potrebama korisnika i u dogovoru sa korisnikom. U poglavlju dizajna opisane su osnovne funkcionalnosti rješenja, zahtjevi za hardverom i softverom, opis i karakteristike klijentskog certifikata, opis korisničkih računa, preporuke za klijentske i serverske certifikate, opis procesa za izdavanje klijentskih certifikata te preporuke za implementaciju. U završnom radu su opisani konfiguracijski parametri na serverskoj i klijentskoj infrastrukturi te izvještaji koji su se razvili za potrebe rješenja problema i izvještaja koji pružaju uvid u korištenje sustava. Opisana su i objašnjenja kodova grešaka zajedno sa preporukama što napraviti u određenoj situaciji. Klijentska strana rješenja sadrži opise zajedno sa konfiguracijskim parametrima.

Ključne riječi: rješenje za automatsko izdavanje certifikata, IRED (engl. *Infrastructure Request Enrollment Distribution*, skraćeno IRED), infrastruktura javnih ključeva (engl. *Public Key Infrastructure*, skraćeno PKI), certifikati.

Abstract

Organizations have been developing information systems, adapting and improving business processes, thus enabling a more efficient and effective organization management. Software Vendors like Microsoft, Oracle, Apple and others are delivering finished solutions that are implemented on a large number of users and they are implemented by system integrations in organizations. Such finished solutions can be configured with options, settings and Out-of-the-box functionalities that are already embedded in the product, but finished solutions cannot be customized, to a greater extent, to the specific needs of organizations. To address specific organization requirements, independent software vendors have developed specialized solutions tailored to organizational needs. One of these custom solutions is described in this final paper. Described are the organization's requirements and the goals for developing and implementing the solution. The solution is designed according to customer's specific needs. Chapter describes the basic functionalities of the solution, hardware and software requirements, description and features of the client certificates, description of user accounts, client and server certificate recommendations, description of the process for issuing the client certificates and deployment recommendations. The final paper describes the configuration parameters on the server and client infrastructure, reports that have been developed for problem solving and the reports that's provide insight into system usage. Error Codes will be explained along with recommendations on what to do in a particular situation. The client side of the solution is described together with the configuration parameters.

Keywords: Certificate Autoenrollment Solution, IRED, Infrastructure Request Enrollment Distribution, Public Key Infrastructure, certificates

1. Sadržaj

2. Uvod

Korisnik kreće u smjeru iskorištavanja digitalnih certifikata za provjeru autentičnosti (engl. *Authentication*) i identifikaciju klijenata. Poslovna jedinica klijenta zahtjeva certifikate za Windows računala kako bi se klijenti potvrdili (engl. *Authenticate*) i identificirali Web aplikacijama. Iako su korisnička računala dio imeničkog direktorija (engl. *Active Directory*, skraćeno AD), računala ne koriste domenske korisničke račune, već koriste lokalne korisničke račune i time se ne mogu iskoristiti prednosti koje pruža inherentna Microsoft Windows funkcionalnost za automatsko izdavanje certifikata. Postojeće web aplikacije imaju zahtjeve za pristup koje klijenti moraju ispuniti. Kako bi se omogućio pristup web aplikacijama odlučeno je da se krene s razvojem specijaliziranog *rješenja za automatsku instalaciju certifikata* prema potrebama korisnika.[1]

Korisnik želi razvoj novog rješenja koje će emulirati zadani (engl. *Default*) proces za automatsko izdavanje certifikata na Microsoft Windows platformi. Pred razvoj rješenja postavili su slijedeći ciljevi i funkcionalnosti:[1]

- Serveri za izdavanje certifikata izdaju klijentske certifikate *IRED* serverima
- *IRED* sustav predaje klijentske certifikate krajnjim korisnicima
- Klijentski certifikati automatski se obnavljaju prema konfiguriranim parametrima
- Politike se provode centralizirano
- Događaji o zahtjevima i instalaciji klijentskih certifikata se bilježe u sustavu
- *IRED* rješenje prikazuje izvještaje o zahtjevima i instalacijama klijentskih certifikata
- *IRED* rješenje u svom radu koristi *imenički direktorij*
- Izuzetno jednostavno korištenje softvera sa klijentske strane
- Rješenje je bazirano na regijama
    - Izvještaji se rade po regijama
    - Mogu se primjenjivati različite politike bazirane po regijama

[1] Span d.o.o., Statement of Work. Zagreb: Krešimir Kovačević, 2011.

3. Obuhvat rješenja

U ovom poglavlju biti će opisan obuhvat *rješenja za automatsko izdavanje certifikata*. Više detalja o rješenju biti će opisano u poglavlju dizajna. Opsegom projekta je obuhvaćen razvoj i implementacija *rješenja za automatsko izdavanje certifikata* kako bi se klijentska računala mogla *potvrditi* i identificirati web aplikacijama. Krajnji ishod projekta je izvršena implementacija IRED servera i razvijena klijentska aplikacija koja je spremna za distribuciju. Prilikom definiranja obuhvata rješenja prikupljeni su inicijalni korisnički zahtjevi koji su sadržani u ovom poglavlju.

Rješenjem za automatsko izdavanje certifikata obuhvaćeno je slijedeće:[2]

- Izrada dizajna rješenja
- Razvoj serverske aplikacije (*IRED*)
- Razvoj klijentske aplikacije
- Razvoj dnevnika događaja i izvještajnog sustava
- Implementacija serverske infrastrukture
- Testiranje sustava na klijentskom računalu

Kako bi se moglo izraditi *rješenje za automatsko izdavanje certifikata* potrebno je izraditi dizajn koji će minimalno sadržavati slijedeće:[2]

- Odrediti smještaj *IRED* servera
- Odrediti *IRED* servere zajedno sa klijentima koje će opsluživati
- Odrediti zahtjeve za *infrastrukturu javnih ključeva* i njihove servere
- Tipovi certifikata koji trebaju biti smješteni na serversku i klijentsku infrastrukturu uzimajući u obzir lokalnu *infrastrukturu javnih* ključeva i *AD* domene
- Odrediti potrebne portove za funkcionalan rad rješenja

Rješenjem za automatsko izdavanje certifikata obuhvaćena je izrada slijedećih izvještaja:[2]

- Izvještaji o greškama
- Sumarni izvještaj
- Mogućnost slanja izvještaja putem e-mail sustava

Rješenjem za automatsko izdavanje certifikata nije obuhvaćeno:[2]

---

[2] Span d.o.o., Statement of Work. Zagreb: Krešimir Kovačević, 2011.

- Rješavanje problema u radu web aplikacija
- Ručna ili automatska instalacija klijentske aplikacije na klijentska računala
- Instalacija certifikata na klijentsko računalo za domenske korisničke račune

Kako bi se moglo pristupiti implementaciji *rješenja za automatsko izdavanje certifikata* potrebno je da klijent pripremi slijedeće:[3]

- Pripremiti serversku infrastrukturu. Instalaciju i konfiguraciju servera izvršiti prema specifikaciji servera
- Dostaviti potrebne instalacijske ključeve za softver
- Instalirati i konfigurirati antivirusni softver na serverska računala
- Otvoriti potrebne portove
- Pripremiti *infrastrukturu javnih ključeva*
- Klijentska računala moraju imati instaliran odgovarajući lanac certifikata od strane lokalne *infrastrukture javnih ključeva* kojem vjeruju
- Pružiti potrebne informacije o klijentskoj infrastrukturi i pridruženim *IRED* serverima
- Pripremiti testno klijentsko računalo

Osnovni koncept *rješenja za automatsko izdavanje certifikata* je opisano u slijedećim točkama:[3]

- Klijentska aplikacija instalirana je kao Windows servis koji se pokreće pod lokalnim sistemskim računom
- Klijentsko računalo poziva *IRED* server pružajući mu potrebne informacije za zahtjev ili obnovu certifikata
- *IRED* server zahtjeva certifikat od lokalnog servera za izdavanje certifikata
- Nakon primanja certifikata od strane *infrastrukture javnih ključeva*, *IRED* server smješta klijentski certifikat u lokalnu bazu servera i šalje ga klijentskom računalu koje je iniciralo zahtjev
- Klijentski certifikat instalira se pod lokalnim korisničkim računom
- Prilikom instalacije certifikata i brisanja starog certifikata, klijentsko računalo šalje potvrdnu poruku prema *IRED* serveru kako bi *IRED* server mogao zabilježiti taj događaj.

[3] Span d.o.o., Statement of Work. Zagreb: Krešimir Kovačević, 2011.

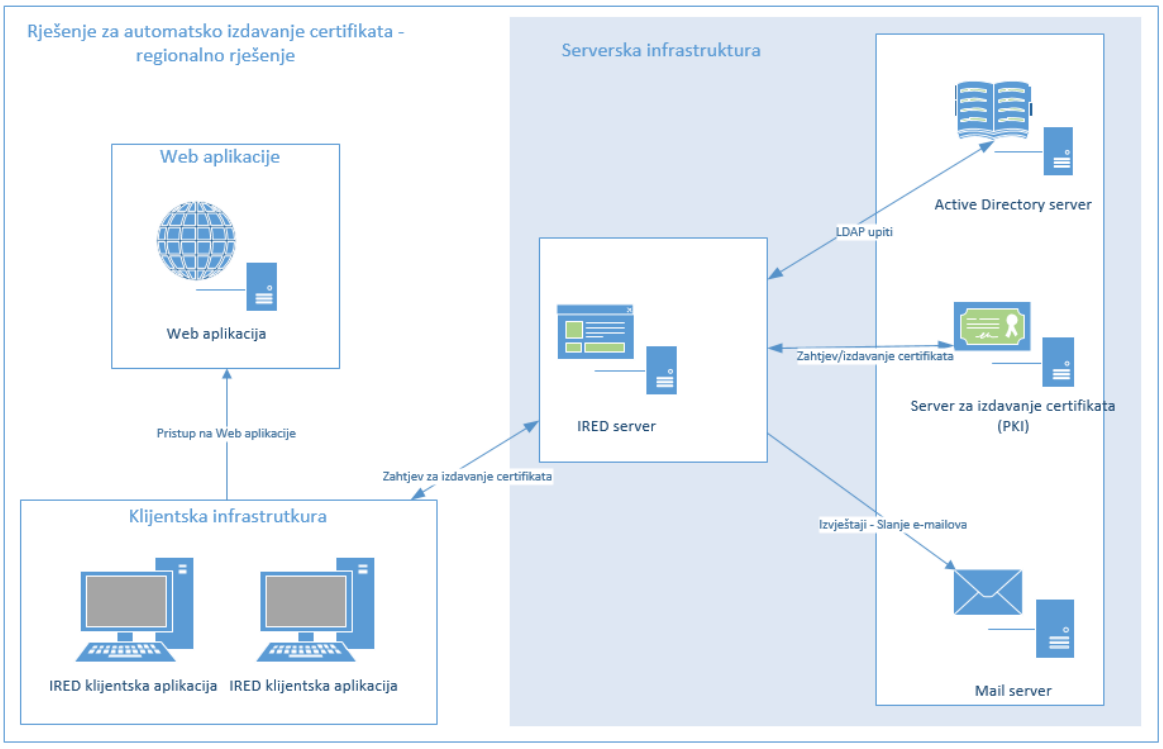
- Jednom dnevno, provjerava se definirana vrijednost predloška za certifikate (engl. *Certificate Template*) i trenutna verzija lokalnog korisničkog certifikata. Cilj ove provjere je osigurati da klijentski certifikat odgovara ispravnom *predlošku za certifikate*. Ukoliko je *predložak certifikata* različit, biti će zahtjevan novi certifikat
- Jednom dnevno ili češće, Windows servis klijentske aplikacije provjerava istek certifikata trenutnog korisnika računala
- Ukoliko certifikat ističe u manje od N dana, zahtjeva se obnova certifikata
- Ukoliko se pojavi greška na klijentskom računalu prilikom instalacije klijentskog certifikata, poruka o grešci se šalje *IRED* serveru kako bi se događaj mogao zabilježiti i kako bi se certifikat na *IRED* serveru mogao zadržati. Certifikat se zadržava na *IRED* serveru kako bi se prilikom slijedećeg zahtjeva, iniciranog od strane istog klijentskog računala, mogao pružiti isti certifikat. Ovim načinom je osigurano da je jedan klijentski certifikat izdan i instaliran na klijentsko računalo

4. Dizajn

U poglavlju dizajna opisati će se osnovne funkcionalnosti rješenja, promjene u dizajnu za vrijeme trajanja projekta, zahtjevi za hardverom i softverom, opis klijentskog certifikata, opis korisničkih računa, preporuke za klijentske i serverske certifikate, opis procesa za izdavanje certifikata, preporuke za implementaciju, regionalni serveri i klijenti, opis potrebnih portova i zahtjevi za *infrastrukturu javnih ključeva*.

Rješenje za automatsko izdavanje certifikata je bazirano na regijama i potrebno je da svaka regija ima svoj *IRED* server. Svakom *IRED* serveru je potrebna lokalno instalirana Microsoft SQL baza i SQL izvještajni (engl. *Reporting*) servis.

Odnos serverske i klijentske infrastrukture prikazan je na slici (Slika 4.1).



Slika 4.1 Odnos serverske i klijentske infrastrukture

4.1. Osnovne funkcionalnosti rješenja

Rješenje za automatsko izdavanje certifikata emulira Windows automatski proces za izdavanje certifikata.

Promjene u dizajnu. Prema inicijalnom zahtjevu postojalo je jedno ograničenje koje je bilo potrebno promijeniti. Inicijalno je predviđeno da se klijentska aplikacija instalira kao Windows servis na klijentsko računalo i da će se klijentski certifikati izdavati samo lokalnim korisničkim računima. Tijekom projekta ukazala se potreba za korištenjem domenskih korisničkih računa na klijentskim računalima, odnosno da je potrebno izdati klijentske certifikate domenskim korisničkim računima. Windows servis obavlja funkciju instalacije klijentskog certifikata samo za lokalni korisnički račun, ali ne i za domenski korisnički račun istog imena iz razloga što su to dva korisnička računa. Kako bi se certifikat mogao instalirati u lokalno skladište za certifikate, Windows servis mora znati lokalno korisničko ime i lozinku korisničkog računa. Windows servis ne može instalirati certifikat bez imena i lozinke lokalnog korisničkog računa. Kako bi se unaprijedilo rješenje klijentska aplikacija neće biti instalirana kao Windows servis već kao klijentska aplikacija. Klijentska aplikacija će se pokretati u kontekstu korisnika. Prednosti ovog scenarija opisane su dolje navedenom:

- Lozinka (engl. *Password*) – Nije potrebno znati lozinku korisničkih računa.
- Domenski korisnički računi – *IRED* rješenje funkcionira sa lokalnim korisničkim računima računala i sa domenskim korisničkim računima.
- Dinamična konfiguracija – Na serverskoj strani sustava se konfiguriraju korisnički računi koji imaju pravo pristupa i izdavanja klijentskih certifikata, kao i koliko često će se provjeravati klijentski certifikati.
- Jednostavniji razvoj – Nije potrebno predstavljati korisnika za izdavanje certifikata.

Osnove koncepta. Iako su osnove koncepta *rješenja za automatsko izdavanje certifikata* opisane u prethodnom poglavlju, u ovom poglavlju će biti ponovno opisane sa više detalja, uzevši u obzir izmjene tijekom razvoja[4]

- Klijentska aplikacija (*IRED*) je instalirana u Program Files direktoriju.
- Klijentska aplikacija ima konfiguracijski file u kojem je specificiran URL od *IRED* servera.
- Klijentska aplikacija se starta i traži parametre trenutnog korisnika (engl. *Current User*) i ime računala (engl. *Machine Name*).
- *IRED* web servis provjerava da li korisnik ima prava za izdavanje klijentskog certifikata

[4] Span d.o.o., Change Request. Zagreb: Krešimir Kovačević, 2012.

    - Ukoliko korisnik nema prava za izdavanje klijentskog certifikata, klijentska aplikacija se gasi.
    - Ukoliko korisnik ima prava za izdavanje *IRED* certifikata, *IRED* klijentska aplikacija dalje provjerava *predložak za certifikate.*
- Klijentska aplikacija se brine da su klijentski certifikati ažurni i validni
    - Ukoliko korisnik ima valjan klijentski certifikat aplikacija čeka N sati za ponovni pokušaj izdavanja klijentskog certifikata.
    - Ukoliko korisnik nema valjani klijentski certifikat, aplikacija zahtjeva certifikat i instalira ga u *lokalno korisničko skladište* (engl. *Local User Store*).
- U slučaju bilo kakvih grešaka, kao što je dohvaćanje konfiguracije sa *IRED* servera ili grešaka prilikom instalacije klijentskog certifikata, klijentska aplikacija zaustavlja svoj rad na N minuta i nakon N minuta pokušava ponovno poslati zahtjev za izdavanjem klijentskog certifikata.
- Određene aktivnosti na sustavu su logirane u *dnevniku događaja* (engl *Event Log*, skraćeno EV) lokalnog računala i u serverskoj bazi.
- Izvještaji – potrebno je razviti izvještaje koji će pomoći pri rješavanju problema i dati uvid u korištenje sustava. Definirani su izvještaji koji će sadržavati slijedeće:
    - Izvještaje o greškama.
    - Sumarni izvještaj koji sadržava zahtjeve za izdavanjem klijentskih certifikata i koji bilježi instalirane certifikate.
    - Izvještaji se mogu poslati putem *protokola za slanje e-mail poruka* (engl. *Simple Mail Transfer Protocol*, skraćeno SMTP).

Općeniti zahtjevi koji su se postavili pred razvoj rješenja[5]

- Osigurati dedicirane *IRED* servere. Na *IRED* serverima neće biti instaliranih aplikacija ili servisa za druge namjene.
- *IRED* server mora biti dio Microsoft *imeničkog direktorija* zajedno sa serverom za izdavanje certifikata iz lokalne *infrastrukture javnih ključeva*.
- Klijentska računala moraju vjerovati kompletnom lancu certifikata lokalne *infrastrukture javnih ključeva*.

[5] Span d.o.o., Design. Zagreb: Krešimir Kovačević, 2012.

- Osigurati dedicirani imenički korisnički račun za izdavanje klijentskih certifikata. Korisnički račun će biti korišten od strane *IRED* servera i *infrastrukture javnih ključeva*.

4.2. Zahtjevi za hardverom i softverom

Prije implementacije *rješenja za automatsko izdavanje certifikata* potrebno je ispuniti preduvjete i zahtjeve za hardverom i softverom na klijentskoj i serverskoj infrastrukturi. Ukoliko nisu ispunjeni svi preduvjeti i zahtjevi, mogući su problemi u radu sa rješenjem. Za navedene verzije softvera osigurati će se ispravno funkcioniranje sustava i moći će se pružiti podrška od strane proizvođača softvera. Ukoliko se ukaže potreba za novim verzijama softvera, kao npr. nova verzija Microsoft SQL servera, potrebno je napraviti sveobuhvatne testove cjelokupnog rješenja. Sveobuhvatni testovi trebaju potvrditi ispravnost pojedinih komponenti sustava i da li je potrebno razvijati nove verzije softvera.

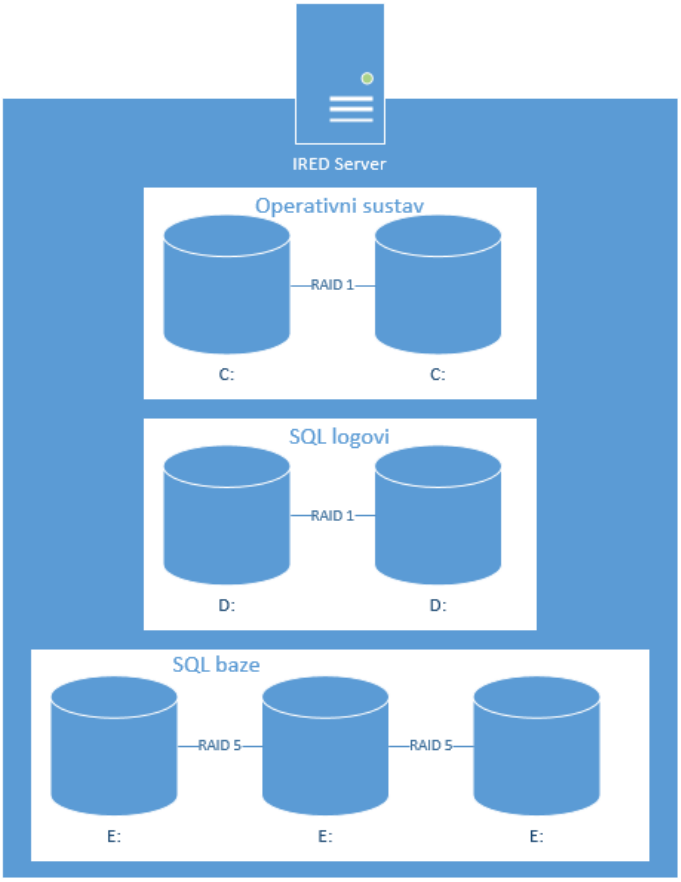
Serverski hardverski zahtjevi – Potrebno je osigurati tri servera slijedećih karakteristika.[6]

- Serverski poslužitelji mogu biti virtualni ili fizički
- Centralni procesor (engl. *Central Processing Unit*, skraćeno CPU) – 2,5 GHz, 4 procesorske jezgre
- Radna memorija (engl. *Random-access memory*, skraćeno RAM) – 16 GB
- Diskovni prostor
    - Sistemsko diskovno polje: 80 GB za Windows operativni sustav
    - Diskovno polje za logove: Minimalno 20 GB, Optimalno 40 GB za SQL logove
    - Diskovno polje za bazu: Minimalno 40 GB, Optimalno 80 za SQL bazu

Dizajn diskovnog sustava servera – Ukoliko se *IRED* serveri instaliraju na fizičke servere, preporuka je da se odvoje diskovi za operativni sustav, logove i baze. *Redundantno polje neovisnih diskova* (engl. *Redundant Array of Independent Disks*, skraćeno RAID) kategorije 1 preporučeno je polje za operativni sustav i logove od SQL baze. RAID 1 polje osigurava podatke i povećava performanse diskovnog sustava. U slučaju pada jednog diska, drugi disk će nastaviti normalno raditi. Neispravan disk potrebno je što prije zamijeniti.

[6] Span d.o.o., Design. Zagreb: Krešimir Kovačević, 2012.

Redundantno polje neovisnih diskova (engl. *Redundant Array of Independent Disks*, skraćeno RAID) kategorije 5 preporučeno je polje za pohranu SQL baze podataka. RAID 5 polje osigurava podatke od mogućih gubitaka i povećava kapacitet logičkog diskovnog polja u odnosu na RAID 1. U slučaju pada jednog od diskova u RAID 5 polju, ostali diskovi će nastaviti normalno raditi (Slika 4.2). Neispravan disk je potrebno što prije zamijeniti.



Slika 4.2 Diskovna polja servera

Softverski zahtjevi za *IRED* server - Kako bi se *IRED* serverska aplikacija mogla instalirati i ispravno funkcionirati, potrebno je ispuniti slijedeće preduvjete:[7]

- Operativni sustav - Microsoft Windows Server 2008 R2 Standard Edition ili Microsoft Windows Server 2012 R2 Standard Edition
- SQL baza podataka - Microsoft SQL 2008 R2 Standard Edition ili Microsoft SQL 2012 Standard Edition
- Izvještajni servis - Microsoft SQL Reporting Service
- IIS 7.x ili viši

[7] Span d.o.o., Design. Zagreb: Krešimir Kovačević, 2012.

- .Net Framework 4.x

Ukoliko softverski preduvjeti nisu ispunjeni, neće biti moguće instalirati *IRED* serversku aplikaciju.

Drugi softverski zahtjevi i preporuke - *IRED* serveri će biti dostupni velikom broju klijenata i potrebno je voditi brigu o sigurnosti i dostupnosti rješenja kako ne bi bilo prekida u radu servisa. Preporuka je da se na servere instalira antivirusno rješenje, uspostavi nadzor i backup servera. Antivirusno rješenje na serveru bi štitilo server od malicioznog koda dok bi se sa nadzorom servera mogao vršiti reaktivni i pro-aktivni nadzor servera. Uspostavom redovitog backupa servera spriječio bi se mogući gubitak podataka u slučaju katastrofa. U tu svrhu preporuka je instalirati i konfigurirati slijedeće softvere na servere:[8]

- Antivirusni klijent – Symantec Endpoint Protection
- Backup - Microsoft DMP
- Nadzor servera - Microsoft SCOM

Ispunjenjem navedenih zahtjeva i preporuka, problemi u radu bi se mogli riješiti brže i kvalitetnije. Cilj je osigurati dostupnost usluge kako korisnici sustava ne bi imali prekida u svome radu.

Zahtjevi za kontrolnim domenskim serverom (engl. *Domain Controller*, skraćeno DC) – *IRED* server u svom radu koristi imeničke resurse i stoga je potrebno na lokaciji *IRED* servera imati implementiran lokalni *kontrolni domenski server*. *IRED* server bi domenske upite slao direktno lokalnom *kontrolnom domenskom serveru*.[8]

Potrebna prava – Za instalaciju serverske *IRED* aplikacije potrebno je imati lokalna administratorska prava i *imenički korisnički račun* (engl. *Active Directory Account*) koji ima prava na predviđenom *predlošku za certifikate*. [8]

Softverski zahtjevi za klijentsku aplikaciju – Kako bi se klijentska aplikacija mogla instalirati na klijentsko računalo potrebno je ispuniti slijedeće preduvjete: [8]

- Operativni sustav za radne stanice - Microsoft Windows XP ili Microsoft Windows 7
- .Net Framework 3.5 SP1

[8] Span d.o.o., Design. Zagreb: Krešimir Kovačević, 2012.

Ukoliko softverski preduvjeti nisu ispunjeni klijentska aplikacija neće moći izvršiti instalaciju na klijentsko računalo.

4.3. Klijentski certifikat

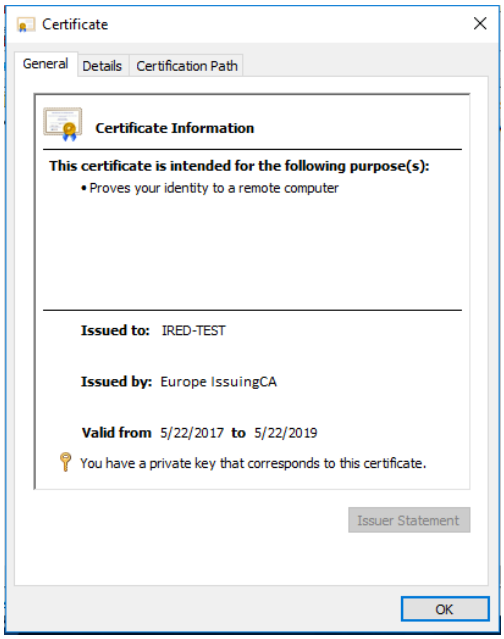
Kako bi klijentska računala odnosno korisnici mogli pristupiti, identificirati i ovjeriti (engl. *Authentication*) se specifičnim web aplikacijama, potrebno je imati instalirani klijentski certifikat određenih karakteristika. Iako su računala dio *imeničkog direktorija*, klijentski certifikati su instalirani unutar korisničkog računa lokalnog korisnika.

Značajke *IRED* klijentskog certifikata su slijedeće:[9]

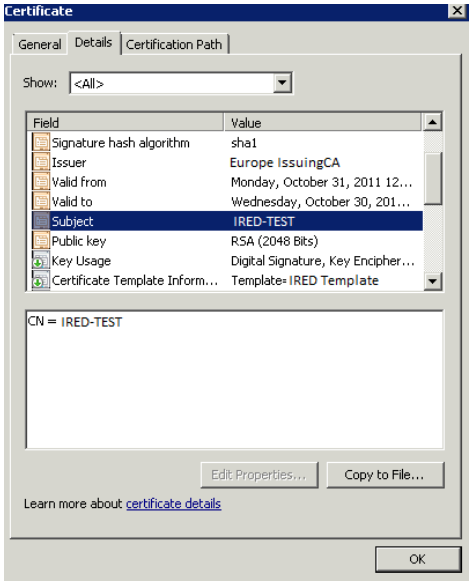
- Klijentski certifikat je instaliran u *lokalno korisničko skladište* (engl. *Local User Store*).
- Ime subjekta u klijentskom certifikatu sadrži *osnovni mrežni ulazni/izlazni sustav* (engl. *Network Basic Input/Output System*, skraćeno NetBIOS) ime lokalnog računala.
- Klijentski certifikati su izdani od strane servera za izdavanje certifikata koji je dio lokalne *infrastrukture javnih ključeva*.
- Klijentski certifikati su izdani iz IREDTemplate *predloška za certifikate*.
- Samo jedan korisnički certifikat je prisutan za trenutnog korisnika (engl. *CURRENT_USER*).

Primjer izdanog klijentskog certifikata možemo vidjeti na slikama (Slika 4.3 i Slika 4.4).

[9] Span d.o.o., Design. Zagreb: Krešimir Kovačević, 2012.



Slika 4.3 Primjer izdanog klijentskog certifikata – opće kratice



Slika 4.4 Primjer izdanog klijentskog certifikata - detalji

Na slikama klijentskog certifikata možemo primijetiti ime servera za izdavanje certifikata, predmet (engl. *Subject*) certifikata sadrži upisano *NetBIOS* ime računala i druge parametre. Dio upisanih parametara su ujedno bili i zahtjevi koji su se postavili pred razvoj ovog rješenja.

4.4. Klijentski korisnički računi

Kako bi osigurali izdavanje certifikata za samo ovlaštene korisnike, definirani su korisnički računi koji imaju pravo izdavanja certifikata i oni se konfiguriraju na serverskoj strani sustava. Korisnički račun koji ima pravo izdavanja računa zvati ćemo Korisnik.

Tijekom dizajniranja rješenja odlučeno je da se klijentska aplikacija pokreće u kontekstu korisnika (engl. *User*), umjesto kao servis. Prednosti pokretanja aplikacije u kontekstu korisnika su slijedeće:[10]

- Lozinka (engl. *Password*) – Nije potrebno znati lozinku korisničkih računa.
- Imenički korisnički računi – Rješenje funkcionira sa lokalnim korisničkih računima računala i imeničkim korisničkim računima.
- Dinamična konfiguracija – Na serverskoj strani sustava se konfiguriraju korisnički računi koji imaju pravo pristupa i izdavanja certifikata kao i koliko često će se provjeravati certifikati na klijentskoj strani.
- Jednostavniji razvoj – Nije potrebno predstavljati korisnika za izdavanje certifikata.

U ovom scenariju svi korisnici na računalu će moći pokrenuti klijentsku aplikaciju. Nakon pokretanja aplikacije, na serverskoj strani provjerava se da li korisnički račun ima pravo zahtijevanja certifikata. Ukoliko korisnički račun nije na listi korisničkih računa koji imaju pravo zahtijevati certifikat, server odbacuje zahtjev za izdavanje certifikata i klijentska aplikacije se gasi.

4.5. Lanac certifikata na serverskoj i klijentskoj infrastrukturi

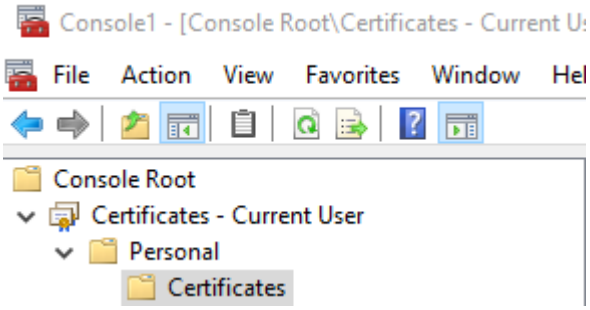
Kako bi rješenje ispravno funkcioniralo potrebno je držati se preporuka za *infrastrukturu javnih ključeva* i certifikate koji se instaliraju iz iste. Preporuke se odnose na lanac certifikata *infrastrukture javnih ključeva* na serverskoj i klijentskoj strani infrastrukture. Certifikati koji se koriste na serverskoj i klijentskoj strani su specifični za pojedino aplikativno korištenje i specifični po načinu kako ih aplikacije koriste. *Infrastruktura javnih ključeva* implementirana na lokaciji će se koristiti za izdavanje serverskih i klijentskih certifikata.

[10] Span d.o.o., Design. Zagreb: Krešimir Kovačević, 2012.

Potrebno je da serveri i klijentska računala vjeruju lancu certifikata lokalne *infrastrukture javnih ključeva*.

Klijentski certifikat – preporuke

- Klijentski certifikat mora biti instaliran iz lokalne *infrastrukture javnih ključeva.*
- Klijentski certifikat mora biti instaliran iz IREDTemplate *predloška za certifikate*.
- Klijentski certifikat mora sadržavati *NetBIOS* ime računala u *predmetu* certifikata.
- Klijentski certifikata mora biti instaliran u osobnom skladištu trenutnog korisnika (Slika 4.5).

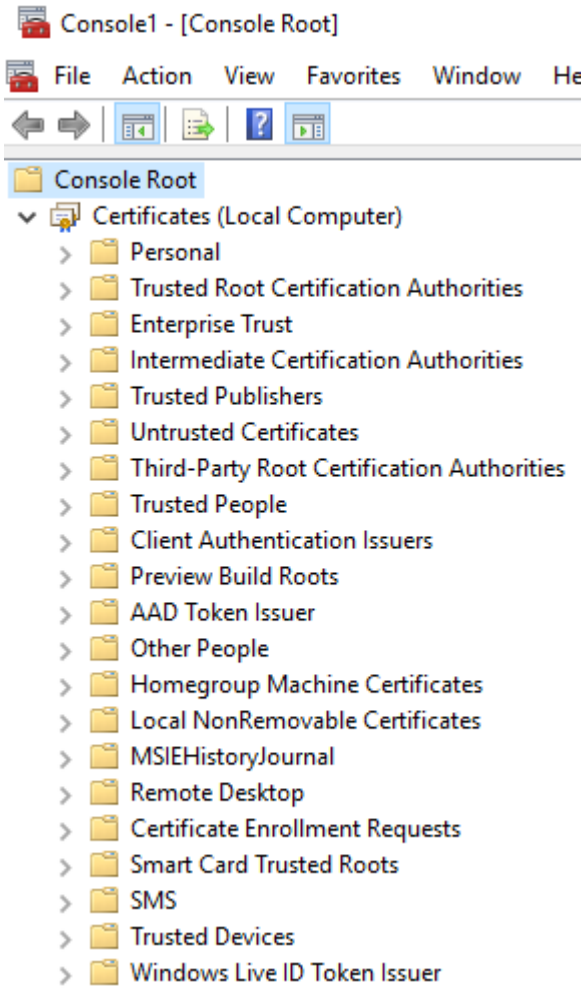


Slika 4.5 Osobno skladište certifikata

Ispravnost lanaca certifikata (engl. *Chain Validation*) **na klijentskoj infrastrukturi**[11]

- *RootCA* certifikat mora biti instaliran na klijentskom računalu u *pouzdanom vršnom tijelu za izdavanje certifikata* (engl. *Trusted Root Certification Authorities*) (Slika 4.6).
- *SubCA* certifikat mora biti instaliran na klijentskom računalu u *središnjem tijelu za izdavanje certifikata* (engl. *Intermediate Certification Authorities*) (Slika 4.6).
- *IssuingCA* certifikat mora biti instaliran na klijentskom računalu u *središnjem tijelu za izdavanje certifikata* (engl. *Intermediate Certification Authorities*) (Slika 4.6).

[11] Span d.o.o., Design. Zagreb: Krešimir Kovačević, 2012.



Slika 4.6 Pouzdano vršno i središnje tijelo za izdavanje certifikata

Serverski certifikat, preporuke za *IRED* web servis

- Serverski certifikat mora biti instaliran iz lokalne *infrastrukture javnih ključeva*
- Serverski certifikat mora biti izdan iz serverskog *predloška za certifikate*

Ispravnost lanaca certifikata (engl. *Chain Validation*) **na serverskoj infrastrukturi**[12]

- *RootCA* certifikat mora biti instaliran na serverskom računalu u *pouzdanom vršnom tijelu za izdavanje certifikata* (engl. *Trusted Root Certification Authorities*) (Slika 4.6).
- *SubCA* certifikat mora biti instaliran na serverskom računalu u *središnjem tijelu za izdavanje certifikata* (engl. *Intermediate Certification Authorities*) (Slika 4.6).

[12] Span d.o.o., Design. Zagreb: Krešimir Kovačević, 2012.

- *IssuingCA* certifikat mora biti instaliran na serverskom računalu u *središnjem tijelu za izdavanje certifikata* (engl. *Intermediate Certification Authorities*) (Slika 4.6).

Lista opozvanih certifikata - preporuke

Potrebno je omogućiti pristup *listi opozvanih certifikata* (engl. *Certificate Revocation List*) *infrastrukture javnih ključeva* za web aplikacijske servere, *IRED* servere i klijentska računala. Lokalna *infrastruktura javnih ključeva* je instalirana kao troslojna arhitektura

- Vršni autoritet za izdavanje certifikata
- Podređeni autoritet za izdavanje certifikata
- Autoritet za izdavanje certifikata krajnjim korisnicima

4.6. Opis procesa za izdavanje certifikata

Kako bi *IRED* sustav ispravno funkcionirao definiran je proces za izdavanje klijentskih *IRED* certifikata. Proces opisuje tijek izdavanja klijentskog certifikata nakon uspješne instalacije *IRED* klijentske aplikacije:[13]

1. *IRED* klijentska aplikacija spaja se na *IRED* server i dohvaća konfiguraciju
    a. Ukoliko *IRED* server nije dostupan pokreće se korak 6 u procesu.
2. Prolazak kroz lokalnu bazu certifikata i validacija svakog klijentskog certifikata sastoji se od slijedećih koraka:
    a. Ukoliko je klijentski certifikat važeći, ali nije izdan od *predloška za certifikate* koji se nalazi u konfiguraciji, klijentski certifikat se dodaje na listu za brisanje.
    b. Ukoliko postoji više od jednog važećeg certifikata izdanog od *predloška za certifikate* koji se nalazi u konfiguraciji, klijentski certifikat ili certifikati koji su stariji se dodaju na listu za brisanje.
    c. Ukoliko klijentski certifikat nije valjan, što uključuje i certifikate za koje se ne može dohvatiti *lista opozvanih certifikata*, dodaje se na listu za brisanje.
3. Ukoliko klijentski certifikat, koji je definiran u konfiguraciji odnosno *predlošku za certifikate*, ne postoji, pokreće se proces pod točkom 3.a. i 3.b.
    a. Zahtjeva se novi klijentski certifikat sa *IRED* web servisa.

[13] Span d.o.o., Client configuration. Zagreb: Stanka Mataga, 2012.

b. Instalira se novi klijentski certifikat u lokalno skladište za certifikate.

Ukoliko jedan od koraka (3.a. i 3.b.) nije uspješan, proces ide na točku 6.

4. Brisanje klijentskih certifikata – brisanje klijentskih certifikata koji su označeni kao nevažeći u koraku 2.
5. Kraj procesa označen kao uspjeh
6. Kraj procesa označen kao greška

Proces validacije certifikata je proces koji se odvija u slijedećim koracima[14]

1. Provjera datuma isteka certifikata (nije ispravan prije i nije ispravan poslije)
2. Validacija *liste opozvanih certifikata* – da li je certifikat opozvan ili *lista opozvanih certifikata* nije dostupna.
3. Validacija serverskih certifikata – *RootCA* je potrebno da bude u lokalnom skladištu *pouzdanog vršnog tijela za izdavanje certifikata* (engl. *Trusted Root Certification Authority*).

4.7. Preporuke za implementaciju

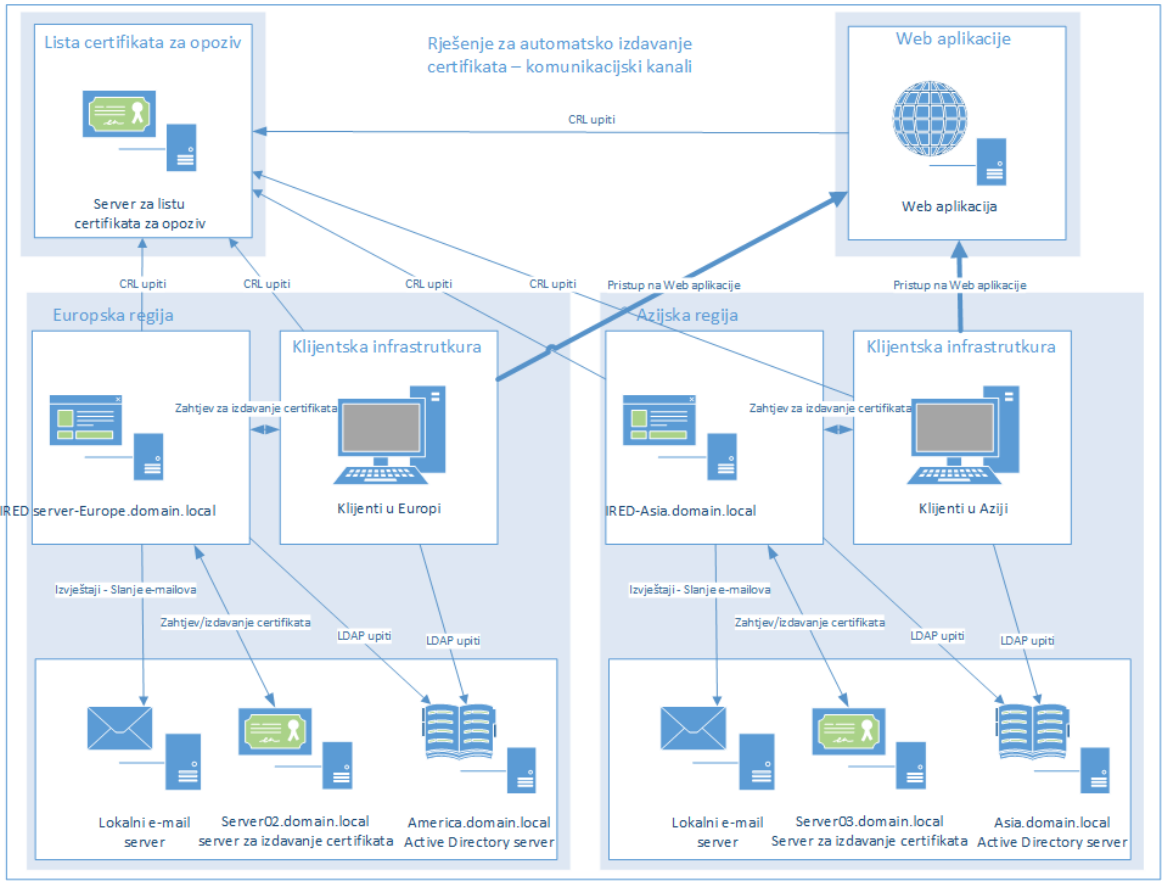
Za potrebe razvoja rješenja potrebno je implementirati razvojnu infrastrukturu gdje će se pisati razvojni kod. Prije nego li se rješenje implementira u produkcijskom okruženju preporuča se rješenje testirati u pred produkcijskom okruženju kako bi se otklonile greške prije puštanja sustava u rad i prije instalacije novih verzija programa. U produkcijskom okruženju potrebno je implementaciju izvršiti kao u tablici (Tablica 4.1**Pogreška! Izvor reference nije pronađen.**).

Za uspješnu implementaciju rješenja potrebno je osigurati slijedeće:

- Otvoriti sve potrebne portove prije implementacije rješenja
- Osigurati funkcionalan AD sustav
- Osigurati funkcionalnu lokalnu *infrastrukturu javnih ključeva* (Tablica 4.3)
- Osigurati servere i dovoljno resursa na serverima
- Osigurati servere po pojedinoj regiji
- Osigurati potrebne serverske i klijentske licence
- Osigurati softver za automatsku instalaciju klijentske aplikacije

[14] Span d.o.o., Client configuration. Zagreb: Stanka Mataga, 2012.

U primjeru (Slika 4.7) možemo vidjeti komunikacijske kanale *IRED* servera sa serverima *infrastrukture javnih ključeva*, komunikaciju klijentskih računala sa *IRED* serverima i aplikativnim serverima za Europsku i Azijsku regiju.



Slika 4.7 Komunikacijski kanali u regionalnoj implementaciji

4.7.1. Regionalni serveri i klijenti

Rješenje za automatsko izdavanje certifikata je bazirano na regijama te pojedini serveri pokrivaju određene regije.

Tablica (Tablica 4.1) prikazuje pojedine *IRED* servere i regije koje opslužuju te *URL*-ove za spajanje klijentskih aplikacija.

Tablica 4.1 Regionalni *IRED* serveri

DNS ime *IRED* servera	Regija	URL
IRED-America.domain.local	Sjeverna Amerika	IRED-America.domain.local

IRED-Europe.domain.local	Europa	IRED-Europe.domain.local
IRED-Asia.domain.local	Azija	IRED-Asia.domain.local

Tablica (Tablica 4.2) prikazuje klijente koji se nalaze unutar pojedine regije zajedno sa AD domenom kojoj pripadaju.

Tablica 4.2 Regionalna klijentska računala

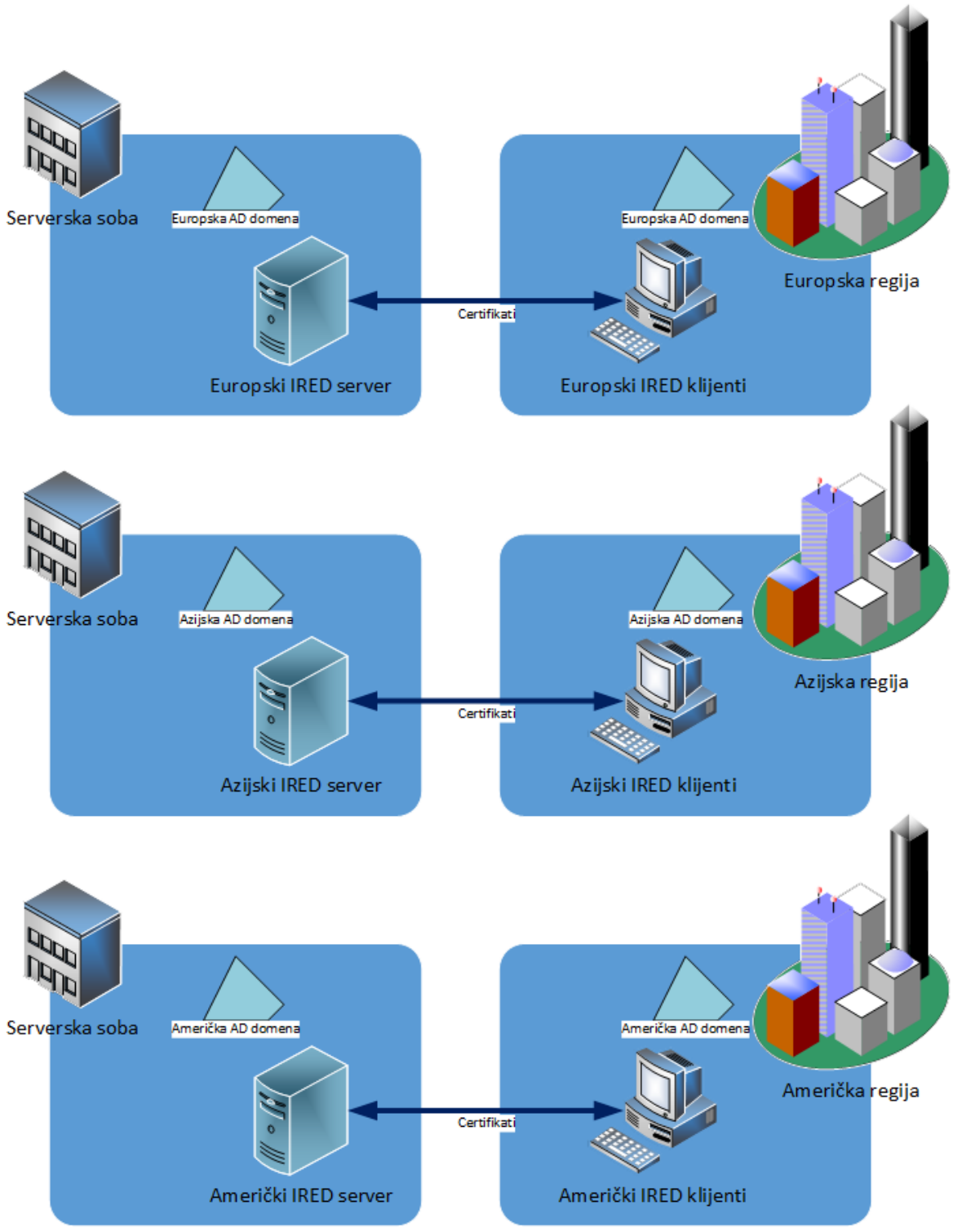
Klijentska računala	Regija	*AD* lokacija
Klijentska računala Sjeverne Amerika	Sjeverna Amerika	america.domain.local
Klijentska računala Europe	Europa	europe.domain.local
Klijentska računala Azije	Azija	asia.domain.local

Regionalni serveri za izdavanje certifikata pružaju klijentske certifikate pojedinim *IRED* serverima koji ih dalje dostavljaju klijentskim računalima. Klijentski certifikati se izdaju iz zajedničkog *predloška za certifikate* (Tablica 4.3).

Tablica 4.3 Regionalni serveri za izdavanje certifikata

Središnje tijelo za izdavanje certifikata klijentima	Regija	Predložak za certifikate
Server01.domain.local	Sjeverna Amerika	IREDTemplate
Server02.domain.local	Europa	IREDTemplate
Server03.domain.local	Azija	IREDTemplate

Na slici (Slika 4.8) možemo vidjeti pojednostavljeni prikaz pojedinog *IRED* servera i regije koje opslužuju zajedno sa njihovim klijentima.[15]



Slika 4.8 Regionalni serveri i klijenti

[15] Span d.o.o., Design. Zagreb: Krešimir Kovačević, 2012.

4.8. Port zahtjevi

Kako bi *rješenje za automatsko izdavanje certifikata* ispravno funkcioniralo potrebno je trajno otvoriti portove od klijenata prema *IRED* serveru i od *IRED* serveru prema drugim sustavima kao što su *imenički direktorij* i serveri za izdavanje certifikata. Klijentska računala se spajaju na web servis *IRED* servera i zahtijevaju klijentski certifikat. Nakon što je klijentsko računalo zatražilo certifikat od *IRED* servera, *IRED* server traži certifikat od servera za izdavanje certifikata po određenim portovima. Nakon dobivanja certifikata *IRED* server prosljeđuje certifikat klijentskom računalu.

Ukoliko određeni klijenti žele pristupiti izvještajnim servisima potrebno je otvoriti portove za pristup istome. S obzirom da je *IRED* server dio *imeničkog direktorija* potrebno je otvoriti portove i prema lokalnim *AD* serverima. Detaljan popis portova i smjer komunikacije se nalazi u tablici (Tablica 4.4).[16]

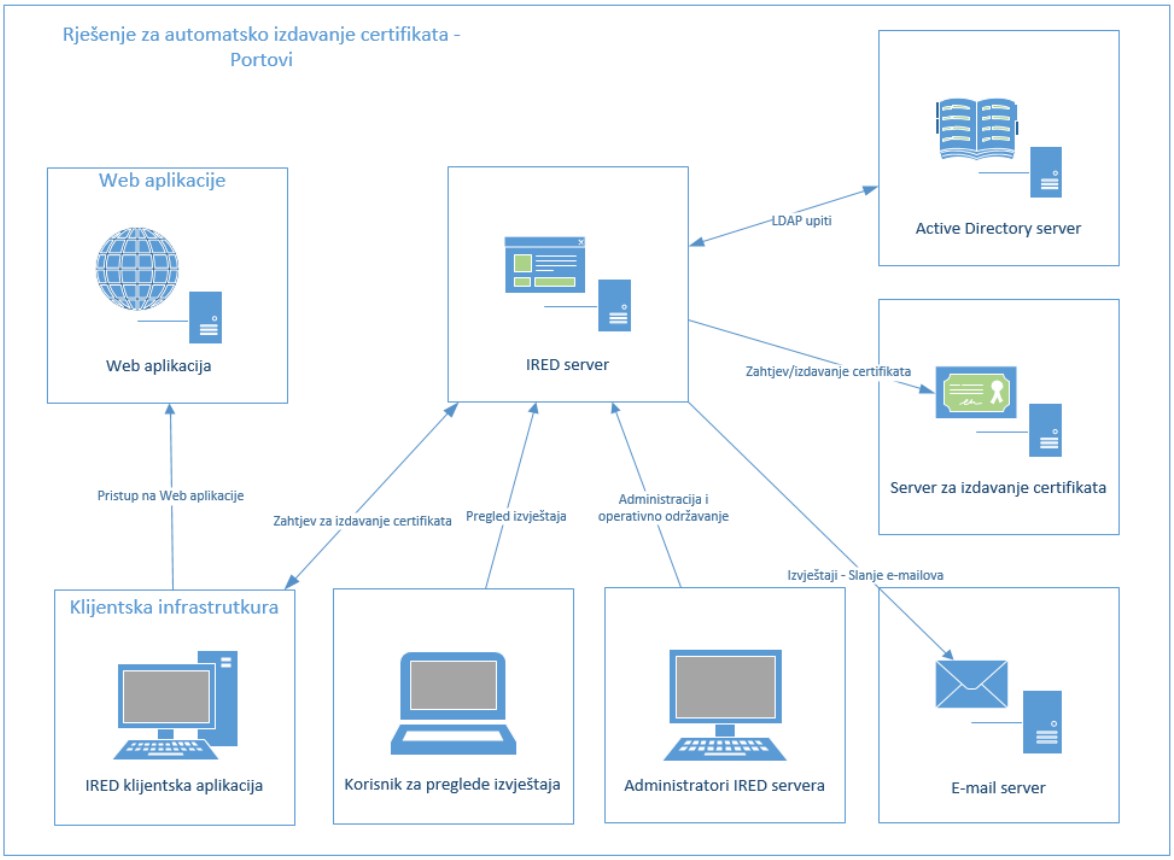
Tablica 4.4 Port zahtjevi

Izvor	Odredište	Transportni protokol	Odredišni port	Komentar
IRED klijent	*IRED* server	TCP	443	Komunikacija *IRED* klijenta prema specifičnom *IRED* serveru. Potrebno za izdavanje certifikata
IRED server	Imenički direktorij	TCP	53, 88, 135, 139, 389, 445, 464, 636, 3268, 3269, 5722, 1024-65535	Komunikacija između *IRED* servera i lokalnih *AD* servera. Lagani upiti imeničkog protokola upiti (engl. *Lightweight Directory Access Protocol*, skraćeno *LDAP*)

[16] Span d.o.o., Design. Zagreb: Krešimir Kovačević, 2012.

IRED server	Imenički direktorij	UDP	53, 67, 88, 123, 137, 138, 389, 464, 636	Komunikacija između *IRED* servera i lokalnih *AD* servera.
IRED server	Server za izdavanje certifikata	TCP	80, 443, 135, 1024-65535	Komunikacija između *IRED* servera i servera za izdavanje certifikat.
IRED server	E-mail server	TCP	25	Komunikacija između *IRED* servera i e-mail servera za potrebe slanja izvještaja putem e-maila
Klijentska računala	*IRED* server	TCP	80, 443	Komunikacija između klijenta i servera za potrebe izrade izvještaja.
Administrator	*IRED* server	TCP/UDP	3389, 80, 443, ICMP	Komunikacija potrebna za pristup i administraciju *IRED* servera.

Shematski prikaz portova se nalazi i u slikovnom prikazu (Slika 4.9).



Slika 4.9 Port zahtjevi

Potrebno je otvoriti portove i za druge preporučene aplikacije kao što su backup, antivirus i softver za nadzor servera.

4.9. Infrastruktura javnih ključeva

Rješenje za automatsko izdavanje certifikata ne izdaje same certifikate već koristi postojeći sustav *infrastrukture javnih ključeva* za izdavanje certifikata. Prije implementacije *rješenja za automatsko izdavanje certifikata* potrebno je dizajnirati i implementirati lokalnu *infrastrukturu javnih ključeva*. S obzirom da *rješenje za automatsko izdavanje certifikata* uvelike ovisi o *infrastrukturi javnih ključeva* potrebno je istu redovito održavati u optimalnom stanju.

4.9.1. Certifikati

Osnovni pojmovi vezani za *infrastrukturu javnih ključeva* su certifikat, autoritet za izdavanje certifikata i *lista opozvanih certifikata*.

- Certifikati su digitalni prikazi računala, korisnika, mrežnog uređaja ili servisa. Certifikati su predstavljeni kao subjekti certifikata.
- Autoritet za izdavanje certifikata (engl. *Certificate Authority*, skraćeno CA) je serversko računalo koje izdaje certifikate korisnicima, računalima ili servisima.
- Lista opozvanih certifikata (engl. *Certificate Revocation List*, skraćeno CRL) je lista opozvanih certifikata od strane servera za izdavanje certifikata.

Certifikati su digitalna prava koja su izdana od servera za izdavanje certifikata i povezana su javnim i privatnim ključem. Certifikat je digitalno potpisan skup informacija. Parametri koje certifikat sadrži su slijedeći:

- Informacije o korisniku ili računalu
- Informacije o serveru koji je izdao certifikat
- Informacije o enkripciji za digitalni potpis
- Informacije o statusu opoziva i pravomoćnosti certifikata

4.9.2. Lista certifikata za opoziv

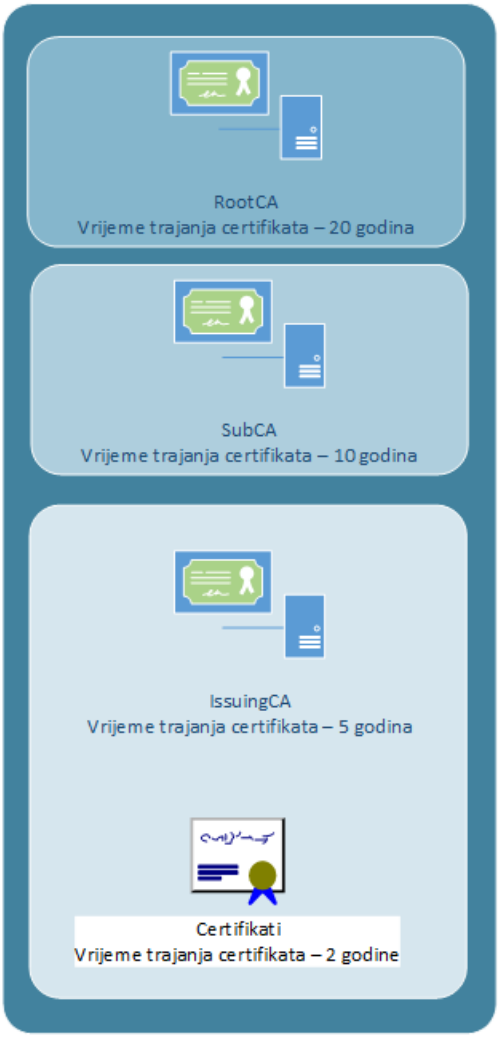
Lista certifikata za opoziv sadrži listu ručno opozvanih certifikata prije isteka perioda njihove pravomoćnosti. Informacije o opozvanom certifikatu sadrže serijski broj certifikata i razlog zbog kojega je certifikat opozvan.

4.9.3. Serveri za izdavanje certifikata

Serveri za izdavanje certifikata imaju na sebi instalirane servise za izdavanje certifikata, provjeravaju identitete korisnika koji zahtijevaju certifikate, izdaju certifikate i upravljaju sa opozivima certifikata.

- Vršni autoritet za izdavanje certifikata (engl. *Root Certificate Authority*, skraćeno RootCA) je najviši autoritet za izdavanje certifikata. *RootCA* certifikati su certifikati koji su samo-izdani. U troslojnom dizajnu *RootCA* izdaje certifikate drugim CA serverima. *RootCA* server je potrebno zaštititi najvišim stupnjem zaštite što uključuje fizičku zaštitu, limitiran pristup te isključenje servera sa lokalne mreže.
- Podređeni autoritet za izdavanje certifikata (engl. *Subordinate Certificate Authority*, skraćeno SubCA) je podređeni CA server i obično se nalazi na drugom sloju CA hijerarhije. Na njemu su definirane politike, pravila i procedure organizacije za sigurnost, provjeru identiteta i upravljanje sa certifikatima.
- Autoritet za izdavanje certifikata krajnjim korisnicima (engl. *Issuing Certificate Authority*, skraćeno IssuingCA) izdaje certifikate korisnicima i računalima. Obično je smješten na trećem sloju CA hijerarhije.

Preporuča se implementirati troslojnu *infrastrukturu javnih ključeva* koja se sastoji od vršnog autoriteta za izdavanje certifikata, podređenog autoriteta za izdavanje certifikata i servera koji služi kao autoritet za izdavanje certifikata krajnjim korisnicima (Slika 4.10). Hijerarhija servera za izdavanje certifikata koja se sastoji od tri servera pruža najviše fleksibilnosti i sigurnosti.



Slika 4.10 Troslojna infrastruktura javnih ključeva

4.9.4. Razdoblje pravomoćnosti

Certifikati su vremenski ograničeni i imaju definirano vremensko razdoblje od kada do kada vrijede. Definira se razdoblje u kojem vrijedi određeni certifikat na svakoj razini *CA* hijerarhije. Potrebno je osigurati dovoljno vremena za obnovu podređenog certifikata i pravilo je da se certifikati obnavljaju na pola vremena razdoblja pravomoćnosti. Ne preporuča se vrijeme pravomoćnosti *RootCA* certifikata duže od 20 godina.

U tablici (Tablica 4.5) predložena su vremenska razdoblja pravomoćnost za servere *infrastrukture javnih ključeva*.

Tablica 4.5 Razdoblje pravomoćnosti

Tip certifikata	Razdoblje pravomoćnosti
RootCA	20 godina
SubordinateCA	10 godina
IssuingCA	5 godina
Klijentski certifikat	2 godine

5. Serverska infrastruktura

Osnovna serverska infrastruktura sustava se sastoji od *IRED* servera, servera namijenjenih za *infrastrukturu javnih ključeva* i *AD* servera. *IRED* server se sastoji od Microsoft SQL servera zajedno sa izvještajnim (engl. *Reporting*) servisima i *IRED* serverske aplikacije.

Kako bi se klijentska računala identificirala određenim web aplikacijama potrebno je da imaju instaliran *IRED* klijentski certifikat. *IRED* rješenje je odgovorno i brine se da klijentska računala imaju instaliran važeći certifikat.[17]

Rješenje je bazirano na regijama i potrebno je da svaka regija ima svoj *IRED* server i svoje servere za izdavanje certifikata koji su dio lokalne *infrastrukture javnih ključeva*. U tablici (Tablica 5.1) možemo vidjeti regije koje serveri pokrivaju, serverska imena, servere koje koriste za izdavanje certifikata i ime *HTTPS* lokacije koje klijenti koriste za spajanje na *IRED* servere.

Tablica 5.1 Serverska IRED infrastruktura

Regija	DNS ime *IRED* servera	Server za izdavanje certifikata	URL
Sjeverna Amerika	IRED-America.domain.local	Server01.domain.local	https://IRED-America.domain.local
Europa	IRED-Europe.domain.local	Server02.domain.local	https://IRED-Europe.domain.local
Azija	IRED-Asia.domain.local	Server03.domain.local	https://IRED-Asia.domain.local

U tablici (Tablica 5.2) su prikazani serveri koji čine lokalnu *infrastrukturu javnih ključeva* zajedno sa prikazanim *DNS* imenima servera, imenima servera koji se koriste u *infrastrukturi javnih ključeva* i funkcijama koje obavljaju.

[17] Span d.o.o., IRED configuration. Zagreb: Stanka Mataga, 2012.

Tablica 5.2 Serverska infrastruktura javnih ključeva

DNS ime servera za izdavanje certifikata	Ime servera u infrastrukturi javnih ključeva	Funkcija certifikata
ServerRootCA	RootCA	*RootCA*
ServerPolicyCA	PolicyCA	*SubordinateCA*
Server01.domain.local	America IssuingCA	*IssuingCA*
Server02.domain.local	Europe IssuingCA	*IssuingCA*
Server03.domain.local	Asia IssuingCA	*IssuingCA*

5.1. Konfiguracija

Konfiguracija *IRED* servera vrši se u clientconfig.config datoteci (Slika 5.1) i u njoj su definirani parametri koji su potrebni za rad *IRED* servera i *IRED* klijenata. Elementi koji se nalaze u konfiguracijskoj datoteci opisani su dalje u tekstu.[18]

- Validni korisnički računi (engl. *ValidUserNames*) – prikazuje korisničke račune koji imaju pravo zahtijevati konfiguracijske postavke.
- *Predložak za certifikate* - Za ispravno definiranje *predloška za izdavanje certifikata* potrebno je konfigurirati ime *predloška za certifikate*, prijateljsko ime i identifikator objekta opcije.
    - Ime *predloška za certifikate* – Ime predloška za izdavanje certifikata od lokalne *infrastrukture javnih ključeva*.
    - Prijateljsko ime (engl. *Friendly Name*) – Prijateljsko ime predloška za izdavanje certifikata
    - Identifikator objekta (engl. *Object identifier*, skraćeno OID) – Identifikator objekta odnosno *predloška za izdavanje certifikata*.
- Ostale akcije certifikata (engl. *UnmachedCertificateAction*) – Ovom postavkom se definira što će se desiti ukoliko postojeći certifikat na klijentskom računalu ne odgovara definiranom *predlošku za certifikate*. Predefinirana opcija je brisanje.

[18] Span d.o.o., IRED configuration. Zagreb: Stanka Mataga, 2012.

- Zadržati (engl. *Keep*) – Ukoliko je postavljena opcija zadržavanja certifikata, svi certifikati koji ne odgovaraju definiranom *predlošku za certifikate* su zadržani.
- Obrisati (engl. *Delete*) – Ukoliko je postavljena opcija brisanja certifikata, svi certifikati koji ne odgovaraju definiranom *predlošku za certifikate* su obrisani.
- Arhivirati (engl. *Archive*) – Ukoliko je postavljena opcija arhiviranja certifikata, svi certifikati koji ne odgovaraju definiranom *predlošku za certifikate* nisu obrisani, već su arhivirani.

- Prag za istek certifikata (engl. *CertificateExpirationThrashold*) – Definira vremenski period kada će klijent zahtijevati obnovu certifikata. Vremenski period je definiran u danima i njegova predefinirana vrijednost iznosi 90 dana.
- *IssuingCA* – Definira server za izdavanje certifikata.
- Vrijeme upita certifikata (engl. *CertificateQueryTime*) – broj minuta nakon kojeg će zahtjev za izdavanje certifikata biti pokrenuto ponovo. Predefinirano vrijeme za novi pokušaj izdavanja certifikata je 480 minuta.
- Vrijeme pokušaja transakcije (engl. *TransactionRetryTime*) – Ukoliko je proces neuspješan, nakon koliko minuta će proces biti pokrenut ponovo. Predefinirano vrijeme za ponovno pokretanje procesa je 5 minuta.

clientconfig.config

```
<?xml version="1.0"?>
<ClientConfiguration xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <UnmatchedCertificateAction>Delete</UnmatchedCertificateAction>
  <CertificateQueryTime>480</CertificateQueryTime>
  <TransactionRetryTime>5</TransactionRetryTime>
  <CertificateExpirationThrashold>90</CertificateExpirationThrashold>
  <ServerDateTime>2016-05-21T02:09:22.5663465-05:00</ServerDateTime>
  <CertificateTemplates>
    <CertificateTemplate>
      <Name>IREDTemplate</Name>
      <FriendlyName>IRED Template</FriendlyName>
      <Oid>1.3.6.2.5.2.311.33.4.4365644.5114176.26780878.36770735.7875643.6.6692747.5144397</Oid>
    </CertificateTemplate>
  </CertificateTemplates>
  <IssuingCA>Server02\Europe IssuingCA</IssuingCA>
</ClientConfiguration>
```

Slika 5.1 Konfiguracijska datoteka servera - primjer

Na primjeru (Slika 5.1) možemo vidjeti primjer konfiguracijske datoteke jednog *IRED* servera. Unutar konfiguracijske datoteke podešeno je slijedeće:

- Brisanje svih ostalih certifikata na klijentskom računalu
- Period ponovnog pokušaja izdavanja certifikata je 480 minuta
- Vrijeme obnove validnog certifikata je 90 dana

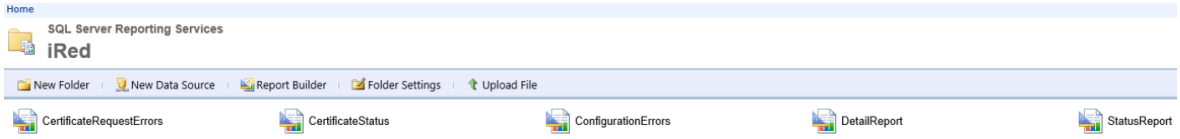
- *Predložak za certifikate* iz kojeg se izdaje certifikat je IREDTemplate sa navedenim OID-om
- *IRED* server koji se koristi je IRED-Europe
- Certifikat je potrebno dohvatiti sa Europe IssuingCA servera za izdavanje certifikata.

Prema korisničkim zahtjevima svi certifikati na klijentskom računalu se brišu osim trenutno izdanog certifikata. Brisanje certifikata je postavljeno kako bi se korisnicima olakšao pristup web aplikacijama, korištenje klijentske aplikacije i računala. Konfigurirati se mogu i druge opcije koje ne brišu postojeće certifikate na klijentskim računalima, kao npr. opcija zadržavanja (engl. *Keep*) svih klijentskih certifikata. Opcija zadržavanja klijentskih certifikata se može koristiti za potrebe testiranja novih verzija aplikacija u razvojnom okruženju.

5.2. Izvještajni sustav

Izvještajni sustav je smješten na serverskoj strani *IRED* sustava i pruža uvid u korištenje i razne događaje sa *IRED* sustavom. Pristup izvještajnom sustavu je dozvoljen samo ovlaštenim osobama. U svrhu rješavanja problema kreirano je 5 slijedećih izvještaja (Slika 5.2):

- Konfiguracijske greške izvještaj (engl. *Configuration Errors*)
- Greške sa izdavanjem certifikata izvještaj (engl. *Certificate Request Errors*)
- Detaljan izvještaj (engl. *Detail Report*)
- Statusi certifikata izvještaj (engl. *Certificate Status Report*)
- Statusni izvještaj (engl. *Status Reports*)



Slika 5.2 Izvještaji

IRED serveri sadrže svoju lokalnu izvještajnu bazu. Pojedinom *IRED* izvještajnom sustavu se može pristupiti preko URL-a koristeći slijedeći link - https://ired.ime.dns.domene/Reports/Pages/Folder.aspx

Opisi izvještaja su opisani u narednim poglavljima.

5.2.1. Izvještaj o konfiguracijskim greškama

Izvještaj o konfiguracijskim greškama (engl. *Configuration Errors*) prikazuje sve događaje odnosno grešake tijekom zahtjeva za konfiguracijom. Greške ovog tipa mogu se pojaviti ukoliko korisničko ime nije na listi odobrenih korisničkih imena. Prilikom izrade izvještaja korisnik može odabrati vremensko razdoblje za koje želi prikazati izvještaj i opcionalno ime određenog klijentskog računala. Parametri za odabir prikazani su na slici (Slika 5.3).[19]

Slika 5.3 Konfiguracijske greške – odabir parametara

Izrađeni izvještaj sadrži kolone kao što su IP adresa klijenta, ime računala, korisničko ime, datum kada se događaj desio, poruka i ime statusa.

5.2.2. Izvještaj o greškama kod izdavanjem certifikata

Izvještaj o greškama kod izdavanja certifikata (engl. *Certificate Request Errors*) prikazuje greške koje se pojavljuju prilikom izdavanja certifikata i na koje klijentsko računalo se odnose. Prilikom izrade izvještaja korisnik može odabrati vremensko razdoblje za koje želi prikazati izvještaj kao i ime određenog klijentskog računala. Parametri za odabir su prikazani na slici (Slika 5.4).[19]

Slika 5.4 Greške sa izdavanjem certifikata – odabir parametara

Izrađeni izvještaj sadrži kolone IP adresa klijenta, ime radne stanice, korisničko ime, datum i vrijeme te poruku i ime statusa. Primjer izrađenog izvještaja možemo vidjeti na slici (Slika 5.5). Na primjeru izvještaja možemo vidjeti klijentsko računalo imena Racunalo55 koje je iniciralo zahtjev za izdavanjem certifikata, ali certifikat nije uspješno instaliran. U drugom

[19] Span d.o.o., IRED configuration. Zagreb: Stanka Mataga, 2012.

primjeru možemo primijetiti klijentsko računalo imena Racunalo11 i zabilježen problema sa instalacijom certifikata. Računalo11 nije uspjelo instalirati certifikat.

From To
10/01/2017 - 10/30/2017

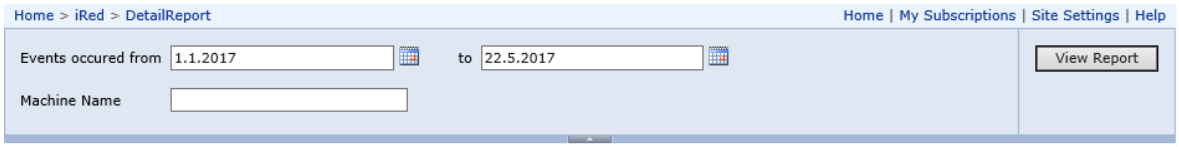
Total rows: 5

Client IP	Machine Name	Username	Date	Message	Status Name
192.168.0.11	Racunalo11	.\Korisnik	10/11/2017 4:28:27 PM	Certificate installation error for .\Korisnik@Racunalo11: The underlying connection was closed: An unexpected error occurred on a receive.	ClientError
192.168.0.22	Racunalo22	.\Korisnik	10/12/2017 9:16:40 PM	Certificate installation error for .\Korisnik@Racunalo22: The operation has timed out	ClientError
192.168.0.33	Racunalo33	.\Korisnik	10/13/2017 1:25:01 AM	Certificate installation error for .\Korisnik@Racunalo33: The operation has timed out	ClientError
192.168.0.44	Racunalo44	.\Korisnik	10/14/2017 6:40:40 PM	Certificate installation error for .\Korisnik@Racunalo44: The operation has timed out	ClientError
192.168.0.55	Racunalo55	.\Korisnik	10/15/2017 1:57:17 AM	GetCertificate initiated	Initiated

Slika 5.5 Greške sa izdavanjem certifikata - primjer izvještaja

5.2.3. Detaljan izvještaj

Detaljan izvještaj (engl. *Detail Report*) prikazuje sve izdane klijentske certifikate u određenom vremenskom periodu. Kao što je prikazano za slici (Slika 5.6), korisnik može odabrati vremenski period i opcionalno računalo za koje želi da se izvještaj prikaže. Parametri za odabir su prikazani na slici (Slika 5.6).[20]



Slika 5.6 Detaljan izvještaj – odabir parametara

Primjer detaljnog izvještaja sadrži kolone kao što je klijentska IP adresa, ime računala, korisničko ime, datum događaja, datum zahtijevanja certifikata, ime subjekta, ime predloška za certifikate i datum isteka certifikata (Slika 5.7).

[20] Span d.o.o., IRED configuration. Zagreb: Stanka Mataga, 2012.

From 10/01/2017 - To 10/30/2017

Total rows: 9

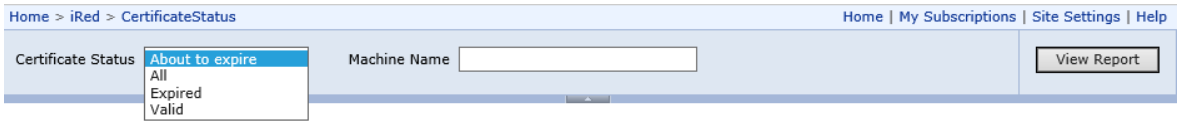
Client IP	Machine Name	Username	Event Date	Certification Request Date	Subject Name	Template	Expiration Date
192.168.0.11	Racunalo11	.\Korisnik	10/30/2017 12:04:10 AM	10/30/2017 12:04:10 AM	CN=Racunalo11	IREDTemplate	3/19/2018 7:50:55 PM
192.168.0.22	Racunalo22	.\Korisnik	10/30/2017 12:15:32 AM	10/30/2017 12:16:18 AM	CN=Racunalo22	IREDTemplate	5/16/2018 9:44:30 PM
192.168.0.33	Racunalo33	.\Korisnik	10/30/2017 12:16:34 AM	10/30/2017 12:16:45 AM	CN=Racunalo33	IREDTemplate	5/16/2018 9:44:30 PM
192.168.0.44	Racunalo44	.\Korisnik	10/30/2017 12:19:11 AM	10/30/2017 12:20:12 AM	CN=Racunalo44	IREDTemplate	12/10/2018 8:34:50 AM
192.168.0.55	Racunalo55	.\Korisnik	10/30/2017 12:20:48 AM	10/30/2017 12:22:22 AM	CN=Racunalo55	IREDTemplate	9/19/2018 2:32:01 AM
192.168.0.66	Racunalo66	.\Korisnik	10/30/2017 12:20:54 AM	10/30/2017 12:21:55 AM	CN=Racunalo66	IREDTemplate	11/14/2018 10:55:31 AM
192.168.0.77	Racunalo77	.\Korisnik	10/30/2017 12:23:30 AM	10/30/2017 12:24:34 AM	CN=Racunalo77	IREDTemplate	4/18/2018 2:21:35 AM
192.168.0.88	Racunalo88	.\Korisnik	10/30/2017 12:28:09 AM	10/30/2017 12:28:10 AM	CN=Racunalo88	IREDTemplate	5/8/2018 3:48:37 PM
192.168.0.99	Racunalo99	.\Korisnik	10/30/2017 12:28:58 AM	10/30/2017 12:28:59 AM	CN=Racunalo99	IREDTemplate	5/16/2018 9:44:30 PM

Slika 5.7 Detaljan izvještaj – primjer izvještaja

U primjeru izvještaja možemo vidjeti da računalo Racunalo22 ima ispravan certifikat i da je datum istjecanja certifikata 16.5.2018 godine.

5.2.4. Izvještaj o statusu certifikata

Izvještaj o statusu certifikata (engl. *Certificate Status Report*) prikazuje sve certifikate koji su izdani klijentskim računalima. Korisnik može filtrirati rezultate po certifikatima koji će uskoro isteći, certifikatima koji su istekli, certifikatima koji su valjani i pregledati sve certifikate neovisno o statusu. Korisnik opcionalno može odabrati ime određenog klijentskog računala. Parametri za odabir su prikazani sa slici (Slika 5.8).[21]



Slika 5.8 Statusi certifikata izvještaj – odabir parametara

[21] Span d.o.o., IRED configuration. Zagreb: Stanka Mataga, 2012.

Izrađeni izvještaj sadrži kolone kao što su IP adresa klijenta, ime klijentskog računala, ime subjekta u certifikatu, ime *predloška za certifikate* i datum istjecanja certifikata. U primjeru izvještaja za certifikate koji su istekli (Slika 5.9), možemo vidjeti da je za Računalo11 certifikat istekao 25.5.2017 godine.

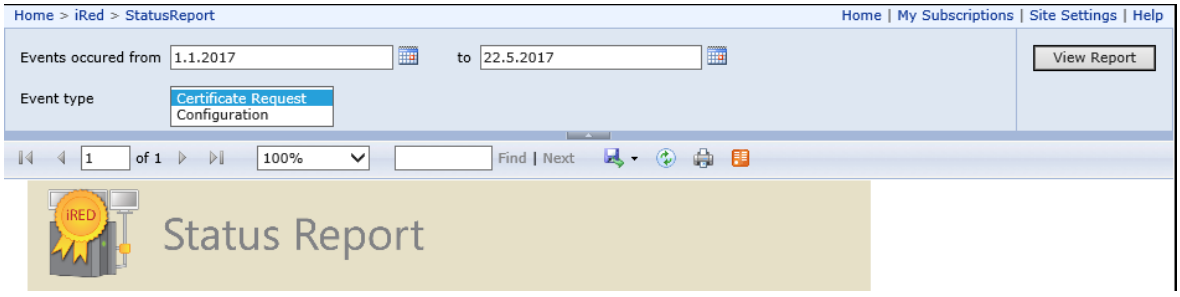
Total rows: 5

Client IP	Machine Name	Subject Name	Template	Expiration Date
192.168.0.11	Racunalo11	CN=Racunalo11	IREDTemplate	5/25/2017 5:35:52 PM
192.168.0.22	Racunalo22	CN=Racunalo22	IREDTemplate	5/25/2017 5:36:48 PM
192.168.0.33	Racunalo33	CN=Racunalo33	IREDTemplate	6/1/2017 8:26:02 PM
192.168.0.44	Racunalo44	CN=Racunalo44	IREDTemplate	10/25/2017 9:15:01 AM
192.168.0.55	Racunalo55	CN=Racunalo55	IREDTemplate	10/25/2017 9:42:37 AM

Slika 5.9 Statusi certifikata – primjer izvještaja

5.2.5. Statusni izvještaj

Statusni izvještaj (engl. *Status Reports*) – Prikazuje događaje filtrirane po tipu (zahtjevi za certifikatima i konfiguracije) i grupirani su po datumima događaja i njihovim statusima. Parametri za odabir prikazani su na slici (Slika 5.10).[22]



Slika 5.10 Statusni izvještaj – odabir parametara

[22] Span d.o.o., IRED configuration. Zagreb: Stanka Mataga, 2012.

Izrađeni izvještaj sadrži kolone kao što su tip događaja, datum događaja, status događaja i broj događaja. Na primjeru izvještaja *zahtjevi za certifikatima* (engl. *Certificate Request*) (Slika 5.11) možemo vidjeti da je 1.1.2017 godine uspješno instalirano 432 certifikata na klijentska računala, dok se 1.4.2017 desila jedna greška prilikom zahtjeva za izdavanjem certifikata.

From To

01/01/2017 - 10/30/2017

Total rows: 12

Event Type	Event Date	Event Status	Events
Certificate Request	01/01/2017	Confirmed	432
Certificate Request	02/01/2017	Confirmed	442
Certificate Request	03/01/2017	Confirmed	433
Certificate Request	04/01/2017	Confirmed	450
Certificate Request	04/01/2017	ClientError	1
Certificate Request	12/01/2017	Confirmed	463
Certificate Request	13/01/2017	Confirmed	446
Certificate Request	13/01/2017	Initiated	2
Certificate Request	13/01/2017	ServerError	1
Certificate Request	14/01/2017	Initiated	1
Certificate Request	14/01/2017	ClientError	2
Certificate Request	14/01/2017	Confirmed	449

Slika 5.11 Statusni izvještaj za zahtjeve certifikata - primjer izvještaja

Na drugom primjeru izvještaja vidimo broj uspješno dostavljenih konfiguracija na klijentska računala po danima (Slika 5.12).

From		To
01/01/2017	-	10/30/2017

Total rows: 196

Event Type	Event Date	Event Status	Events
Configuration	01/01/2017	Delivered	1078
Configuration	02/01/2017	Delivered	1109
Configuration	03/01/2017	Delivered	1092
Configuration	04/01/2017	Delivered	1114
Configuration	05/01/2017	Delivered	1088
Configuration	06/01/2017	Delivered	1116

Slika 5.12 Statusni izvještaj za dostavu konfiguracija – primjer izvještaja

6. Klijentska infrastruktura

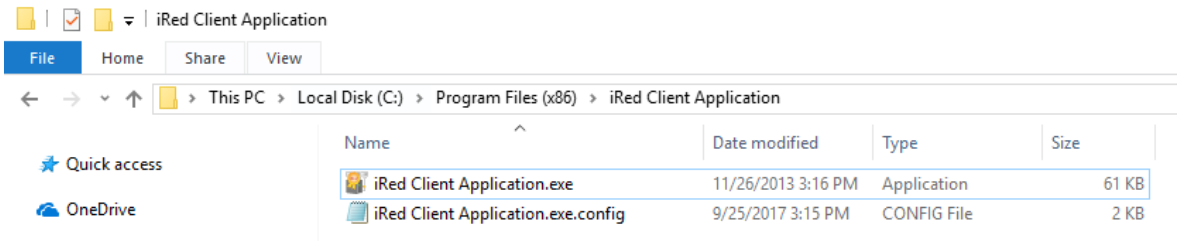
Rješenje za automatsko izdavanje certifikata je bazirano na regijama i sva klijentska računala unutar jedne regije se spajaju na određeni *IRED* server. Svaka regija ima svoj klijentski instalacijski paket koji se koristi pri instalaciji aplikacije na klijentsko računalo. Tablica (Tablica 6.1) prikazuje klijentske aplikacijske pakete koji se instaliraju po određenim regijama i koji serveri su zaduženi za njih.[23]

Tablica 6.1 Klijentski instalacijski paketi po regijama

Regija	*IRED* server	Klijentski instalacijski paket
Sjeverna Amerika	IRED-America.domain.local	IRED_America.msi
Europa	IRED-Europe.domain.local	IRED_Europe.msi
Azija	IRED-Asia.domain.local	IRED_Asia.msi

6.1. Konfiguracija

Konfiguracija klijentske aplikacije se vrši u *Application.exe.config* konfiguracijskoj datoteci. Unutar datoteke je specificiran URL od regionalnog *IRED* servera zajedno sa drugim klijentskim postavkama. Konfiguracijska datoteka je smještena u *C:\Program Files\iRed Client Application* folderu (Slika 6.1).[23]



Slika 6.1 Instalacijski folder klijentske aplikacije

Primjer konfiguracijskih postavki možemo vidjeti u tablici (Tablica 6.2). Tablica sadrži postavke, vrijednosti koje su podešene na klijentima i opise istih.[23]

[23] Span d.o.o., Client configuration. Zagreb: Stanka Mataga, 2012.

Tablica 6.2 Klijentska konfiguracija

Postavka	Definirana vrijednost	Opis vrijednosti
Pauza za servis u sekundama (engl. *ServiceTimeOutSeconds*)	60	Zadana vrijednost je 60 sekundi. Ukoliko Web servis ne odgovori u roku od 60 sekundi, pojavljuje se pauza (engl. *Timeout*)
Ime dnevnika događaja (engl. *EventLogName*)	iRed	Ime pod kojim se pohranjuju događaji u aplikacijskom dnevniku događaja (Slika 7.1).
Otkloniti neispravnosti (engl. *Debug*)	Isključeno (engl. *False*)	Opcija za potrebe otklanjanja problema u radu sa klijentskom aplikacijom. Zadana vrijednost je isključeno.
Interval zaslona (engl. *SplashScreenInterval*)	10	Zadana vrijednost je 10 sekundi. Definira koliko dugo će se poruka prikazivati na iRed statusnom ekranu (Slika 6.3).
CRL provjera (engl. *CrlCheck*)	Uključeno (engl. *True*)	Definira da li se provjerava *CRL*. Zadana vrijednost je uključena što znači da se *CRL* provjerava.
Parameter Web servera (engl. *iRed_Client_Application_ iRedService_iRedService*)	URL	URL regionalnog *IRED* servera.

Ime pod kojim se pohranjuju događaji vezani za klijentsku aplikaciju je iRed što nam olakšava pretraživanje grešaka koje su se desile u radu sustava (Slika 7.1).

Primjer konfiguracijske datoteke klijentske aplikacije možemo vidjeti na slici (Slika 6.2).

iRed Client Application.exe.config

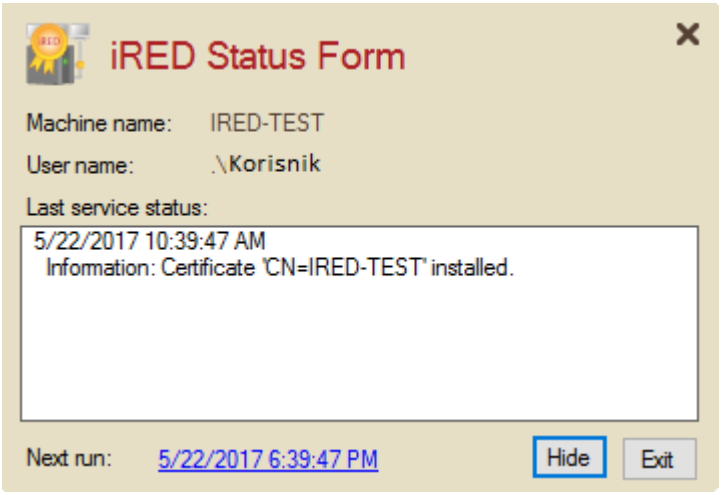
```
<?xml version="1.0"?>
<configuration>
  <configSections>
    <sectionGroup name="applicationSettings" type="System.Configuration.ApplicationSettingsGr
      <section name="iRed.Application.Properties.Settings" type="System.Configuration.ClientS
    </sectionGroup>
  </configSections>

  <applicationSettings>
    <iRed.Application.Properties.Settings>
      <setting name="ServiceTimeOutSeconds" serializeAs="String">
        <value>60</value>
      </setting>
      <setting name="EventLogName" serializeAs="String">
        <value>iRed</value>
      </setting>
      <setting name="Debug" serializeAs="String">
        <value>False</value>
      </setting>
      <setting name="SplashScreenInterval" serializeAs="String">
        <value>10</value>
      </setting>
      <setting name="crlCheck" serializeAs="String">
        <value>True</value>
      </setting>
      <setting name="iRed_Client_Application_iRedService_iRedService" serializeAs="String">
        <value>https://ired-europe.domain.local/iRed/iRedService.asmx</value>
      </setting>
    </iRed.Application.Properties.Settings>
  </applicationSettings>
  <startup>
    <supportedRuntime version="v2.0.50727"/>
  </startup>
</configuration>

```

Slika 6.2 Konfiguracijska datoteka klijentske aplikacije

6.2. Klijentska aplikacija

Nakon pokretanja klijentskog računala, klijentska aplikacija se pokreće automatski. Prilikom pokretanja iRed aplikacije prikazana je *iRed statusna forma* tijekom slijedećih 10 sekundi (ukoliko nije drugačije definirano u konfiguracijskoj datoteci). Primjer statusne forme je vidljiv na slici (Slika 6.3).[24]

[24] Span d.o.o., Client configuration. Zagreb: Stanka Mataga, 2012.

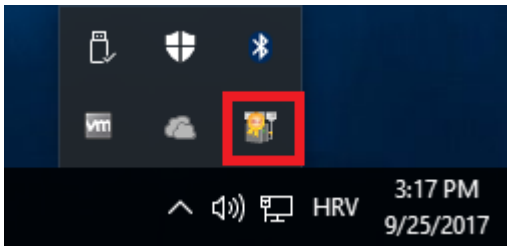


Slika 6.3 Statusna forma klijentske aplikacije

Nakon prolaska *intervala zaslona* (engl. *SplashScreenInterval*), *IRED statusna forma* postaje skrivena. *IRED statusna forma* može biti opet prikazana tako što ju korisnik pozove sa programske trake (engl. *Taskbar*) (Slika 6.4).

Korisnik može ponovno pokrenuti proces izdavanja certifikata tako što odabere link koji prikazuje vrijeme i datum. Link se nalazi pri dnu *IRED statusne forme*, pokraj teksta *ponovno pokretanje* (engl. *Next Run*) (Slika 6.3). Korisnik može sakriti prozor tako što odabere sakrij (engl. *Hide*) gumb (Slika 6.3). Za izlazak iz aplikacije potrebno je odabrati opciju izlazak (engl. *Exit*) (Slika 6.3).

Ukoliko korisnik nije siguran da li je klijentska aplikacija pokrenuta na računalu, pregledom *programske trake* (engl. *Taskbar*) može se utvrditi da li se prikazuje IRED ikona (Slika 6.4). Prikazana *IRED* ikona označava da je aplikacija startana.[25]



Slika 6.4 IRED ikona klijentske aplikacije na programskoj traci

Distribucija klijentske aplikacije – Nakon što su zadovoljeni preduvjeti za instalaciju klijentske aplikacije ista se može instalirati ručno ili automatski. Klijentska aplikacija se može automatski instalirati koristeći softvere za automatsku instalaciju paketa. U slučaju

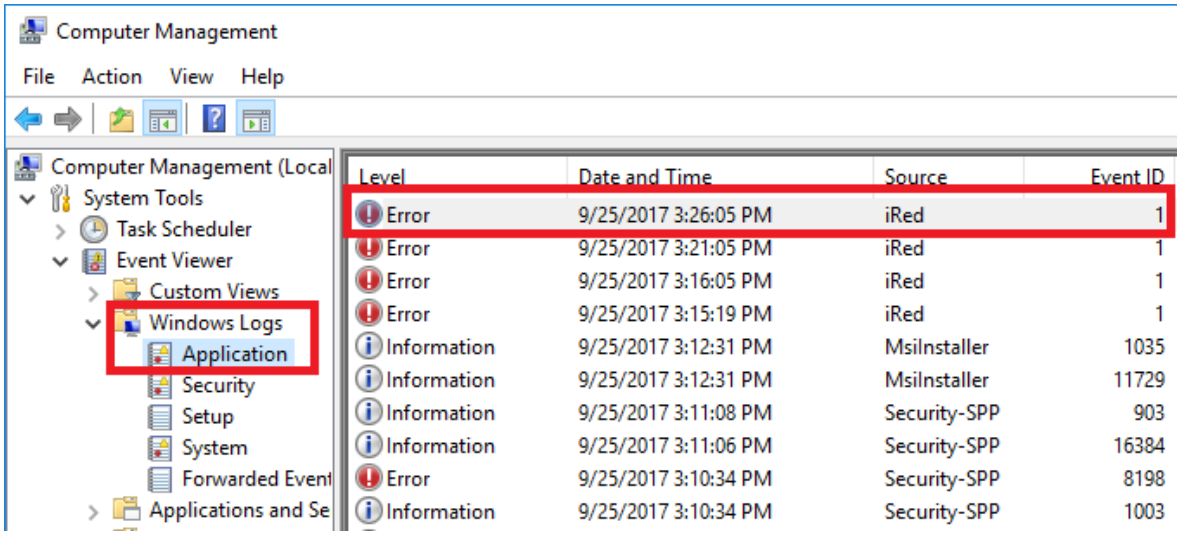
[25] Span d.o.o., Client configuration. Zagreb: Stanka Mataga, 2012.

instalacije aplikacije na veći broj klijentskih računala preporuča se distribucija klijentske aplikacije putem softvera za automatsku instalaciju paketa kao što je Microsoft SCCM.

7. Lista kodova za greške i testiranje sustava

7.1. Lista kodova za greške

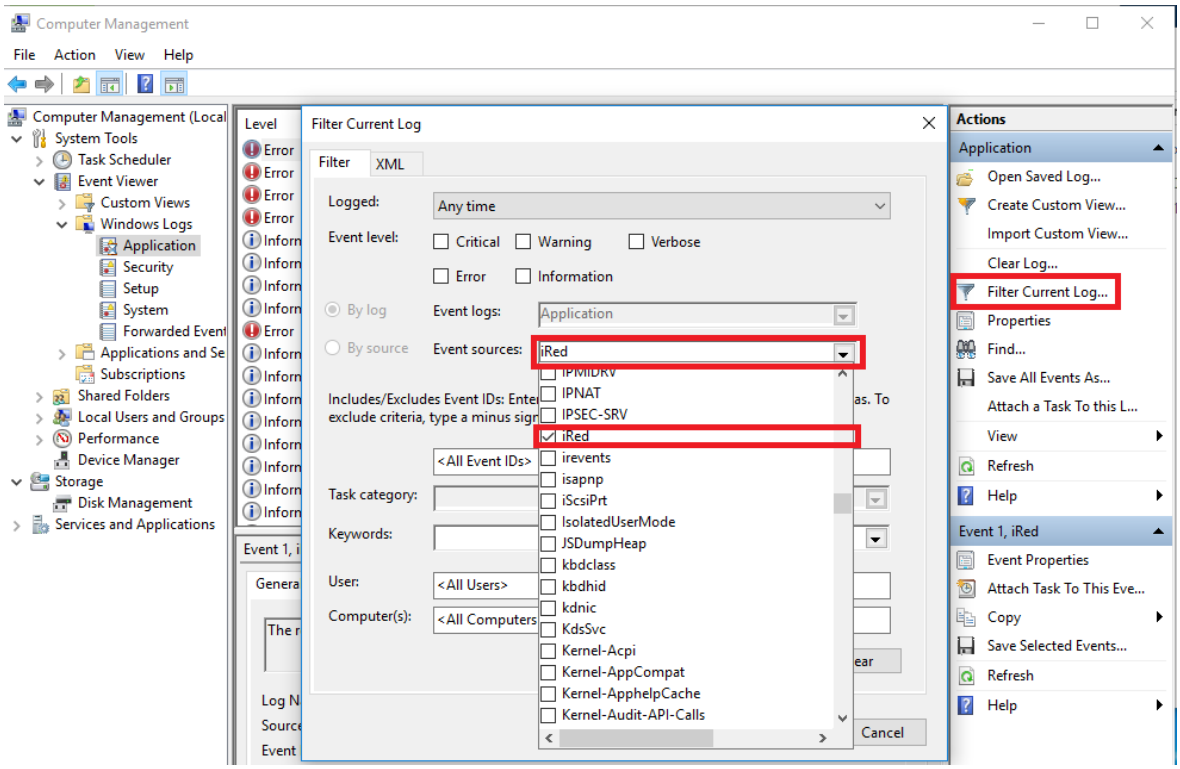
Rješenje za automatsko izdavanje certifikata ima u sebi definiranu listu grešaka koje se mogu pojaviti prilikom korištenja sustava i na temelju kojih se ovlaštenim osobama pruža uvid u određene tipove događaja. Analizom liste grešaka se može odrediti daljnji smjer rješavanja problema. Aktivnosti se bilježe u *dnevniku događaja* na lokalnom računalu (Slika 7.1) i u *IRED* bazi na serverskom računalu.[26]



Slika 7.1 Dnevnik događaja na klijentskom računalu

Ukoliko želimo na klijentskom računalu prikazati samo događaje vezano za *IRED* klijentsku aplikaciju, potrebno je iste filtrirati u dnevniku događaja (Slika 7.2).

[26] Span d.o.o., Client configuration. Zagreb: Stanka Mataga, 2012.



Slika 7.2 Filter dnevnika događaja na klijentskom računalu

Lista grešaka i njihovi opisi se nalazi u tablicama (Tablica 7.1, Tablica 7.2, Tablica 7.3, Tablica 7.4, Tablica 7.5, Tablica 7.6, Tablica 7.7, Tablica 7.8, Tablica 7.9, Tablica 7.10, Tablica 7.11 i Tablica 7.12).[27]

U tablicama su greške izražene engleskim nazivom jer se pod istim nazivom pojavljuju i u *rješenju za automatsko izdavanje certifikata*. Regionalne jezične postavke sustava su razvijene samo za englesko govorno područje.

Tablica 7.1 Lista kodova za greške – događaj 1

Broj događaja	1
Nivo greške	Kritični
Izvor greške	*IRED*
Greška	*iRedServiceUnavailableError*

[27] Span d.o.o., Client configuration. Zagreb: Stanka Mataga, 2012.

Opis događaja	*IRED* servis nije dostupan. *IRED* klijentska aplikacija pokušala je izvršiti spajanje na *IRED* server, ali ga nije uspjela dohvatiti. Razlozi zbog kojih je moglo doći do greške: *DNS* greška (ne može pročitati *DNS* adresu, servis je spušten i drugi razlozi…) Preporuča se provjeriti konekciju između klijenta i servera što uključuje provjeru: ▪ Mrežne konekcije – provjeriti povezivanje sa *IRED* serverom po portu 443 ▪ *DNS-a* – provjeriti dostupnost *DNS* servera. ▪ *IRED* servisa - servis je spušten. Provjeriti da li je *IRED* server u ispravnom stanju.

Tablica 7.2 Lista kodova za greške – događaj 2

Broj događaja	2
Nivo greške	Kritični
Izvor greške	*IRED*
Greška	*iRedServiceUnhandledError*
Opis događaja	*IRED* server ima problema u radu servisa ili postoji greška u razvojnom kodu. Desila se greška na serveru, kontaktirajte odjel podrške.

Tablica 7.3 Lista kodova za greške – događaj 3

Broj događaja	3
Nivo greške	Kritični
Izvor greške	*IRED*
Greška	*CertificateInstalationError*

Opis događaja	*IRED* klijent je primio klijentski certifikat od *IRED* servera, ali ga nije mogao instalirati. Greška se desila na klijentskom računalu tijekom instalacije certifikata. Potrebno je ponovno pokrenuti proces instalacije certifikata koji se sastoji od: 1. Otvoriti *IRED* klijentsku aplikaciju 2. Kliknuti na link pokreni (engl. *Next run*)

Tablica 7.4 Lista kodova za greške – događaj 4

Broj događaja	4
Nivo greške	Kritični
Izvor greške	*IRED*
Greška	*ClientSystemError*
Opis događaja	Sistemska greška se pojavila na strani *IRED* klijenta što može upućivati na grešku u razvojnom kodu (engl. *Bug*). Potrebno je reinstalirati *IRED* klijentsku aplikaciju. Ukoliko problem postoji i nakon reinstalacije klijentske aplikacije potrebno je kontaktirati odjel podrške.

Tablica 7.5 Lista kodova za greške – događaj 5

Broj događaja	5
Nivo greške	Kritični
Izvor greške	*IRED*
Greška	*UserNameNotAlowed*
Opis događaja	Korisnik nije na listi dozvoljenih korisnika. Potrebno je provjeriti korisničkom ime.

Tablica 7.6 Lista kodova za greške – događaj 6

Broj događaja	6
Nivo greške	Kritični

Izvor greške	*IRED*
Greška	*BadPassword*
Opis događaja	Pokušaj izdavanja certifikata korištenjem neispravne lozinke. Mogućnost pristupa *IRED* servisu izvan *IRED* klijenta. Potrebno je utvrditi računalo sa kojeg se pristupa *IRED* serveru i istom onemogućiti pristup *IRED* servisu.

Tablica 7.7 Lista kodova za greške – događaj 7

Broj događaja	7
Nivo greške	Kritični
Izvor greške	*IRED*
Greška	*CATemplateUnavailable*
Opis događaja	Došlo je do konfiguracijske greške. Nije moguće pristupiti *predlošku za certifikate* koji je definiran u konfiguracijskoj datoteci. Potrebno je izvršiti konfiguraciju *IRED* servisa. Kontaktirajte odjel podrške.

Tablica 7.8 Lista kodova za greške – događaj 8

Broj događaja	8
Nivo greške	Kritični
Izvor greške	*IRED*
Greška	*CAIssuingError*
Opis događaja	Certifikat ne može biti izdan *IRED* serveru. Kontaktirajte odjel podrške.

Tablica 7.9 Lista kodova za greške – događaj 9

Broj događaja	9
Nivo greške	Kritični
Izvor greške	*IRED*

Greška	*CAServerStoreError*
Opis događaja	Certifikat ne može biti snimljen ili izbrisan na *IRED* serveru. Potrebno je kontaktirati odjel podrške.

Tablica 7.10 Lista kodova za greške – događaj 10

Broj događaja	10
Nivo greške	Kritični
Izvor greške	*IRED*
Greška	*DBSystemError*
Opis događaja	Baza nije dostupna. Kontaktirajte odjel podrške.

Tablica 7.11 Lista kodova za greške – događaj 11

Broj događaja	11
Nivo greške	Kritični
Izvor greške	*IRED*
Greška	*DBContextError*
Opis događaja	Rekord u bazi nije dostupan. Mogućnost neautoriziranog korištenja *IRED* servisa. Potrebno je otvoriti sigurnosni incident i pristupiti analizi događaja. Kontaktirajte odjel podrške.

Tablica 7.12 Lista kodova za greške – događaj 12

Broj događaja	12
Nivo greške	Kritični
Izvor greške	*IRED*
Greška	*SystemError*

Opis događaja	Sve ostale generičke greške koje se mogu pojaviti. Mogućnost problema sa *IRED* serverom ili je problem u razvojnom kodu. Potrebno je kontaktirati odjel podrške.

Kod analize problema dobro je znati slijedeće:

- Ukoliko se greške od 1 do 4 pojave u dnevniku događaja više od jednom po satu, to može upućivati da su pogrešno definirane postavke ili aplikacija neispravno funkcionira.
- Ukoliko se greške od 5 do 12 pojavljuju na više klijentskih računala, to može upućivati na neispravan rad *IRED* servisa sa serverske strane.

7.2. Testiranje sustava

Kako bi potvrdili uspješnu implementaciju sustava i da se sustav u slučaju nepravilnosti u radu ponaša u skladu sa očekivanjem, izvršeni su slijedeći testovi.

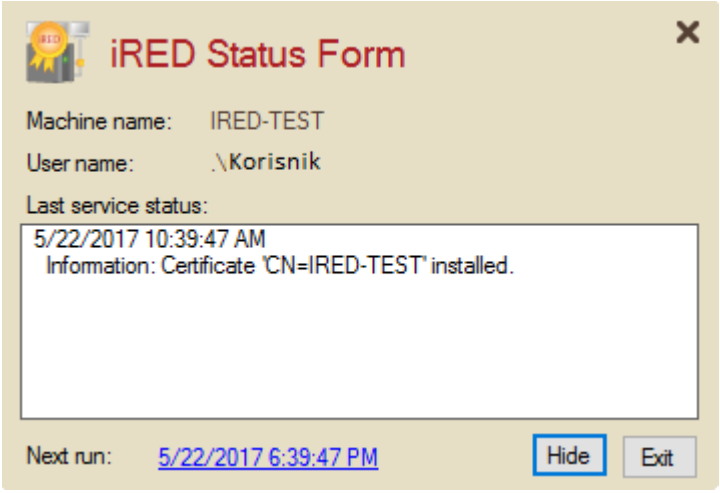
- Test 01 – Izdavanje certifikata
- Test 02 – Klijentska konfiguracijska datoteka
- Test 03 – Ispravnost lanca certifikata
- Test 04 – Neispravan korisnički račun

7.3. Test 01 – Izdavanje certifikata

Cilj testa: Utvrditi ispravnost cjelokupnog *rješenja za automatsko izdavanje certifikata* izdavanjem testnog klijentskog certifikata.

Opis testa: Kako bi se uspješno izdao klijentski certifikat sve komponente sustava moraju ispravno funkcionirati na serverskoj i klijentskoj strani infrastrukture. Iako se test može lako i brzo izvesti sa klijentske strane, test izdavanja certifikata je sveobuhvatan test. Test nam pokazuje da li ispravno funkcionira *infrastruktura javnih ključeva*, *IRED* serverska aplikacija, *IRED* baza podataka, *IRED* klijentska aplikacija, *imenički direktorij* i da su pravilno otvoreni portovi između svih komponenti sustava. Pokrenuto je instaliranje klijentskog certifikata iz klijentske aplikacije.

Očekivani rezultat testa je instaliran klijentski certifikat na klijentsko računalo.



Slika 7.3 Test 01 – Izdavanje certifikata

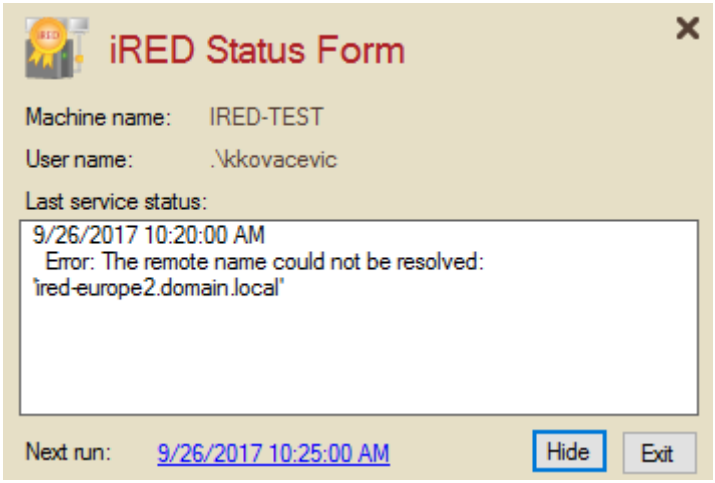
Rezultat testa: Test je evidentiran kao uspješan jer je klijentski certifikat uspješno izdan i instaliran na klijentsko računalo (Slika 7.3).

7.4. Test 02 – Klijentska konfiguracijska datoteka

Cilj testa: Utvrditi pozivanje klijentske konfiguracijske datoteke

Opis testa: U svrhu utvrđivanja pozivanja klijentske konfiguracijske datoteke, konfigurirati će se neispravan *IRED* server. U konfiguracijsku datoteku dodan je nepostojeći *IRED* server.

Očekivani rezultat testa je vraćanje greške klijentske aplikacije prilikom pokušaja kontakta nepostojećeg *IRED* servera.



Slika 7.4 Test 02 – Neispravno ime servera

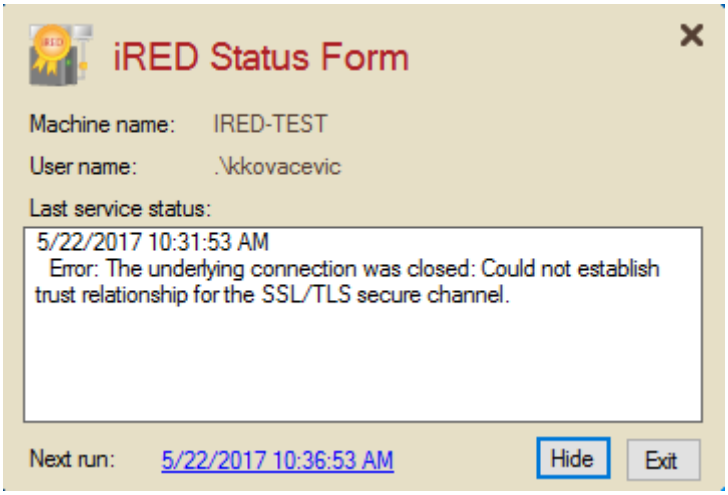
Rezultat testa: Test je evidentiran kao uspješan jer klijentsko računalo nije moglo pronaći *IRED* server (Slika 7.4).

7.5. Test 03 – Ispravnost lanca certifikata

Cilj testa: Utvrditi funkcioniranje *ispravnosti lanca certifikata* (engl. *Chain Validation*)

Opis testa: U svrhu utvrđivanja *ispravnosti lanca certifikata* pokušati će se instalirati klijentski certifikat na klijentsko računalo, ali bez da su se prethodno instalirali certifikati koji čine javni dio serverskog lanca certifikata. Javni dio serverskog certifikata je dio lokalne *infrastrukture javnih* ključeva kojem se vjeruje.

Očekivani rezultat testa je javljanje greške unutar klijentske aplikacije prilikom uspostave povjerljivog odnosa (engl. *Trust relationship*) sa *IRED* serverom i shodno tome klijentski certifikat nije izdan.



Slika 7.5 Test 03 - Neispravan lanac certifikata

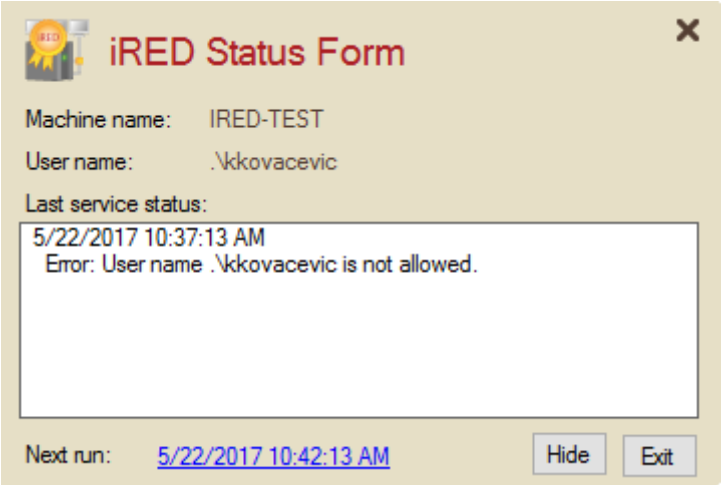
Rezultat testa: Test je evidentiran kao uspješan jer klijentski certifikat nije mogao biti izdan od strane *IRED* servera. Razlog neizdavanja certifikata je nemogućnost uspostavljanja *odnosa povjerenja* za kriptirani transportni protokol (engl. *Secure Sockets Layer*, skraćeno SSL) između klijentskog računala i IRED servera (Slika 7.5).

7.6. Test 04 – Neispravan korisnički račun

Cilj testa: Utvrditi ispravnost liste dozvoljenih korisnika

Opis testa: U svrhu utvrđivanja ispravnosti liste dozvoljenih korisnika kreirati će se korisnički račun na klijentskoj strani kojemu nije dozvoljeno zahtijevanje i dobivanje klijentskog certifikata.

Očekivani rezultat testa je ispisivanje poruke od strane klijentske aplikacije u kojoj stoji da korisnički račun nije dozvoljen. S obzirom da korisnički račun nije dozvoljen neće biti instaliran ni klijentski certifikat.



Slika 7.6 Test 04 - Neispravan korisnik

Rezultat testa: Test je evidentiran kao uspješan jer je klijentska aplikacija ispisala poruku da korisnik nije dozvoljen (Slika 7.6). Klijentski certifikat nije instaliran na klijentsko računalo.

8. Tijek razvoja rješenja i rezultati

Prilikom inicijalnih kontakata sa korisnikom definirani su inicijalni zahtjevi, razlog pokretanja projekta, ciljevi i opseg projekta. Pokretanjem projekta su se dalje definirale uloge i odgovornosti, te preduvjeti koje je potrebno ispuniti za implementaciju. Prvi koraci u projektu su bili izrada dizajna rješenja i priprema serverske infrastrukture. Tijekom izrade dizajna rješenja došlo je do manjih izmjena u funkcionalnostima rješenja kako bi se izradio kvalitetniji sustav. Izmjene su prihvaćene od strane korisnika i izvođača. Nakon definiranja svih stavaka dizajna pristupilo se razvoju izvornog koda. Prva serverska verzija finalnog izvornog koda instalirana je na jedan od pripremljenih regionalnih servera. U međuvremenu klijent je obavio pripremne radove na klijentskoj infrastrukturi i dio pripremnih radova na serverskoj infrastrukturi. Na klijentskoj infrastrukturi provjeren je lanac certifikata i otvoreni su portovi za komunikaciju prema IRED serverima. Na serverskoj strani infrastrukture također je bilo potrebno otvoriti portove za komunikaciju između drugih komponenti sustava. Pripremne radnje uključivale su pripremu *infrastrukture javnih ključeva*, pripremu infrastrukture za distribuciju klijentske aplikacije i pripremne radnje na drugim sustavima. Kako bi se utvrdilo funkcioniranje novog sustava prema dizajnu i utvrdila spremnost za produkciju, dalje su izvršeni testovi koji su potvrdili ispravnost istog. U prvim testovima potvrđena je ispravnost rješenja u testnom okruženju izvođača. U narednim testovima potvrđena je spremnost sustava za produkciju. Nakon uspješno odrađenih testova pristupilo se pripremi klijentske aplikacije za distribuciju. Pripremili su se instalacijski paketi za distribuciju klijentske aplikacije. Distribucija klijentske aplikacije je prvo izvršena na testna računala, te nakon toga i na produkcijska računala. Izvođač je predao klijentsku aplikaciju klijentu i dalje je sve poslove oko distribucije klijentske aplikacije preuzeo klijent i njegovi timovi. Nakon uspješne implementacije *IRED* servera u jednoj regiji pristupilo se implementaciji *IRED* servera u ostalim regijama čime je ispunjen kompletan obuhvat projekta. S obzirom da su isporučene sve stavke i da nakon puštanja sustava u rad nisu uočeni problemi u radu korisnika sustav je predan na održavanje odjelu podrške.

9. Zaključak i analiza

Definirani korisnički zahtjevi nisu mogli biti ispunjeni implementacijom gotovih softverskih rješenja i stoga se pristupilo razvoju novog rješenja koje bi zadovoljilo sve korisničke zahtjeve i ciljeve. *IRED* rješenje je uspješno razvijeno i implementirano na lokaciji korisnika te je potpunosti ispunilo očekivanja. Rješenje je implementirano u produkcijskom i testnom okruženju. U produkcijskom okruženju implementacija je obavljena u više regija. Prema dizajnu rješenja, regionalni serveri opslužuju korisnike koji se nalaze u Sjevernoj Americi, Europi i Aziji. Razdvajanjem sustava na regije omogućilo se organizacijama da uspostave različite politike po pojedinim regijama koje su u skladu sa predviđenim tehničkim rješenjem sustava. Dinamičnom konfiguracijom rješenja povećana je sigurnost sustava na način da se mogu definirati korisnički računi koji imaju pravo pristupa i vjerovati određenom lancu certifikata. Povećanoj sigurnosti doprinijelo je točno definiranje portova za komunikaciju između klijentske i serverske infrastrukture te ostalih dijelova sustava. Otvaranjem samo potrebnih portova se (ograničila osnova) smanjila baza za moguće zlonamjerne napade.

Automatskom distribucijom klijentskog certifikata omogućilo se lakše upravljanje sa sustavom i lakša uspostava potrebnih procesa. Krajnji korisnici ne moraju znati tehnologiju upravljanja i procese za izdavanje i zamjenu certifikata što zahtjeva vrijeme za učenje. Krajnjim korisnicima omogućeno je da se fokusiraju na obavljanje poslova i na stvaranje novih vrijednosti svojim organizacijama. Izrađena je klijentska aplikacija koja ne zahtjeva specijalnu obuku klijenta već klijentska aplikacija radi u pozadini. U slučaju problema korisnici mogu tražiti izdavanje certifikata putem klijentske aplikacije. Dizajnirano je intuitivno sučelje klijentske aplikacije čime se je olakšao rad korisnicima.

Odjelu podrške pružen je uvid u korištenje sustava i olakšano je rješavanje problema u radu sa serverskom i klijentskom infrastrukturom. Razvijeni su izvještaji koji omogućuju lakše adresiranje problema u radu sustava i time se skraćuje potrebno vrijeme za rješavanje problema.

Uspostavljeni su temelji nad kojima se finalno rješenje može proširiti na klijentskoj i/ili serverskoj strani. Postojeća Microsoft aplikacija može se nadograditi novim funkcionalnostima i ukoliko tržište bude zahtijevalo može se razviti aplikacija koja funkcionira na drugim platformama kao što su Cisco, Android, Apple, Linux i drugi.

Popis kratica

IRED	*Infrastructure Request Enrollment Distribution*	Rješenje za automatsko izdavanje certifikata
CPU	Central Processing Unit	Centralni procesor
RAM	Random-access memory	Radna memorija
AD	*Active Directory*	Imenički direktorij
PKI	*Public Key Infrastructure*	Infrastruktura javnih ključeva
CRL	*Certificate Revocation List*	Lista opozvanih certifikata
CA	*Certificate Authority*	Autoritet za izdavanje certifikata
EV	*Event Log*	Dnevnik događaja
DNS	*Domain Name System*	Domenski sustav imena
URL	*Uniform Resource Locator*	Usklađeni lokator sadržaja
SQL	*Structured Query Language*	Strukturirani jezik za upite
IP	*Internet Protocol*	Internetski protokol
SSL	*Secure Sockets Layer*	Kriptirani transportni protokol
ICMP	*Internet Control Message Protocol*	Komunikacijski protokol
SMTP	*Simple Mail Transfer Protocol*	Protokol za slanje e-mail poruka
DC	*Domain Controller*	Kontrolni domenski server
TCP	*Transmission Control Protocol*	Transportni protokol sa kontrolom prijenosa
UDP	*User Datagram Protocol*	Transportni protokol bez kontrole prijenosa
OID	*Object identifier*	Identifikator objekta
LDAP	*Lightweight Directory Access Protocol*	Lagani upiti imeničkog protokola
RAID	*Redundant Array of Independent Disks*	Redundantno polje neovisnih diskova
SCCM	*System Center Configuration Manager*	Centralni sistemski upravitelj konfiguracije
HTTP	*HyperText Transfer Protocol*	Protokol za prijenos hiperteksta

HTTPS	*Hyper Text Transfer Protocol Secure*	Siguran protokol za prijenos hiperteksta
RootCA	*Root Certificate Authority*	Vršni autoritet za izdavanje certifikata
SubCA	*Subordinate Certificate Authority*	Podređeni autoritet za izdavanje certifikata
IssuingCA	*Issuing Certificate Authority*	Autoritet za izdavanje certifikata krajnjim korisnicima
NetBIOS	*Network Basic Input/Output System*	Osnovni mrežni ulazni/izlazni sustav
SCOM	*System Center Operations Manager*	Centralni sustav za operativno upravljanje

Popis slika

Popis tablica

Literatura

[1] Span d.o.o., *Statement of Work*. Zagreb: Krešimir Kovačević, 2011.

[2] Span d.o.o., *Design*. Zagreb: Krešimir Kovačević, 2012.

[3] Span d.o.o., *Change Request*. Zagreb: Krešimir Kovačević, 2012.

[4] Span d.o.o., *IRED configuration*. Zagreb: Stanka Mataga, 2012.

[5] Span d.o.o., *Client configuration*. Zagreb: Stanka Mataga, 2012.

Algebra
visoka škola za
primijenjeno računarstvo

NASLOV DIPLOMSKOG RADA

Pristupnik: Hrvoje Horvat, JMBAG

Mentor: Prof. dr. sc. Dobar Voditelj